	Semana 26/09/2016			
Primary Vendor Product	Usztiption	Published	CVSS Score	Source & Patch Info
aternity aternity	The web server in Aternity 9 and earlier does not require authentication for getMBeansFromURL loading of Java MBeans, which allows remote attackers to execute arbitrary Java code by registering MBeans.	29/09/2016	<u>9.3</u>	CVE-2016-5062
hp network_automation	HP Network Automation Software 9.1x, 9.2x, 10.0x before 10.00.02.01, and 10.1x before 10.11.00.01 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	29/09/2016	<u>7.5</u>	CVE-2016-4385
isc bind	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10 x before 9.10.4-P3, and 9.11 x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.	28/09/2016	<u>7.8</u>	CVE-2016-2776
libgd libgd	Integer overflow in the gitmageWebpCtx function in gd_webp_c in the GO Graphics Ubrary (aka llogd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calis.	28/09/2016	<u>7.5</u>	CVE-2016-7568
redhat jboss_operations_network	The server in Red Hat JBors Operations Network (JON), when SSL authentication is not configured for JON server / agent communication, allows remote attackers to execute arbitrary code via a crafted HTTP request, related to message deserialization. NOT: this vulnerability exists because of an incomplete fix for CVE-506-337.	27/09/2016	<u>9.0</u>	CVE-2016-6330
sap trex	An unspecified function in SAP TREX 7.10 Revision 63 allows remote attackers to execute arbitrary OS commands via unknown vectors, aka SAP Security Note 2203591.	27/09/2016	10.0	CVE-2016-6137
adobe digital_editions	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4263.	26/09/2016	10.0	CVE-2016-6980
citrix linux_virtual_delivery_agent	Citrix Linux Virtual Delivery Agent (aka VDA, formerly Linux Virtual Desktop) before 1.4.0 allows local users to gain root privileges via unspecified vectors.	26/09/2016	7.2	CVE-2016-6276
huawei anyoffice_secureapp	Huawei AnyMail before 2.6.0301.0060 allows remote attackers to cause a denial of service (application crash) via a crafted compressed email attachment.	26/09/2016	7.1	CVE-2016-6826
huawei honor6_firmware	The view driver in Navee Mate 5 smartphones with software CRR-1020 before CRR-1020218362, CRR-1020 before CRR- U120008362, CRR-1020 before CRR-1020538362, and CRR-1220 before CRR-10202538562, P8 smartphones with software GRA- U120008362, CRR-10201886, GRA-1020 before GRA-1020008362, GRA-1020 before CRR-102003866, GRA-C020 before GRA-1020253856, and Honor 6 Plus smartphones with software before 6.9.16 allows attackens to cause a denial of software (Edivare Index) via a crated application.	26/09/2016	<u>71</u>	CVE-2016-8279
lperf_project iperf	The parse_string function in cison.c in the cISON library mishandles UTF8/16 strings, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a non-hex character in a JSON string, which triggers a heap-based buffer overflow.	26/09/2016	<u>7.5</u>	CVE-2016-4303
openssl openssl	Multiple memory leaks in t1 lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to	26/09/2016	7.8	CVE-2016-6304
openssi openssi	cause a denial of service Internerv commention via laree OCSP Status Result extensions. statem/statem_(isis in the OTS implementation in OperaSIS 1.1.0 beforts - Ito allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted DTLS messages.	26/09/2016	7.1	CVE-2016-6308
openssi openssi	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote attackers to cause a denial of service (use-after-free) or possibly execute arbitrary code via a crafted TLS session.	26/09/2016	<u>10.0</u>	CVE-2016-6309
openstack mitaka-murano	OpenStack Murano before 1.0.3 (liberty) and 2.x before 2.0.1 (initials), Murano dashboard before 1.0.3 (liberty) and 2.x before 2.0.1 (initials), Murano dashboard before 1.0.3 (liberty) and 2.x before 2.0.1 (initials), and pythom-muranodient before 0.7.3 (liberty) and 0.8.x before 2.6.5 (initial) improperty use loaders inherited from yani. Loader with partially full files, which a board of 0.8.x before 2.6.5 (initial) improperty use loaders inherited from yani. Loader with partially files of 0.8.x before 2.6.5 (initial) improperty use loaders inherited from yani. Loader with partially files of 0.8.x before 2.6.5 (initial) improperty use loaders inherited from yani. Loader of 0.8.x before 2.6.5 (initial) improperty and 0.8.x before 2.6.5 (initial) improperty use loaders inherited from yani. A state of 0.8.x before 0.7.3 (liberty) and 0.8.x before 0.7.5 (liberty) and 0.8.x before 0.8.5 (initial) improperty use loaders inherited from yani. A state of 0.8.x before 0.7.5 (liberty) and 0.8.x before 0.7.5 (liberty) and 0.8.x before 0.8.5 (initial) improperty use loaders inherited from yani. A state of 0.8.x before 0.7.5 (liberty) and 0.8.x before 0.8.5 (liberty) and 0.8.5 (liber	26/09/2016	<u>7.5</u>	CVE-2016-4972
powerdns authoritative_server	PowerDNS (aka pdns) Authoritative Server before 4.0.1 allows remote primary DNS servers to cause a denial of service (memory exhaustion and secondary DNS server crash) via a large (1) AXFR or (2) IXFR response.	26/09/2016	7.1	CVE-2016-6172
apple apple_tv	ambinary and access to the second of the second sec	25/09/2016	10.0	CVE-2016-4658
apple mac_os_x	The Apache HTTP Server in Apple OS X before 10.12 and OS X Server before 5.2 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrasted CG iclent data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's valued HTTP raffic LO an arbitrary proxy server via a crafted Proxy header in an HTTP request, alsa an "httpoxy" issue, a related issue to CVE-2016-5387.	25/09/2016	<u>75</u>	CVE-2016-4694
apple mac_os_x	AppleEFIRuntime in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app.	25/09/2016	<u>9.3</u>	CVE-2016-4696
apple mac_os_x	Apple HSSPI Support in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4697
apple iphone_os	AppleMobileFileIntegrity in Apple IOS before 10 and OS X before 10.12 mishandles process entitlement and Team ID values in the task port inheritance policy, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	25/09/2016	<u>9.3</u>	CVE-2016-4698
apple mac_os_x	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4700.	25/09/2016	<u>9.3</u>	CVE-2016-4699
apple mac_os_x	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4699.	25/09/2016	<u>9.3</u>	CVE-2016-4700
apple apple_tv	Audio in Apple IOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	25/09/2016	10.0	CVE-2016-4702
apple mac_os_x	Bluetooth in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	<u>9.3</u>	CVE-2016-4703
apple mac_os_x	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4710.	25/09/2016	7.2	CVE-2016-4709
apple mac_os_x	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4709.	25/09/2016	7.2	CVE-2016-4710
apple apple_tv	CoreCrypto in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted app.	25/09/2016	9.3	CVE-2016-4712
apple mac os x	diskutil in DiskArbitration in Apple OS X before 10.12 allows local users to gain privileges via unspecified vectors. Intel Graphics Driver in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a	25/09/2016	7.2	CVE-2016-4716
apple mac_os_x	denial of service (memory council of a scatter and and a scatter and a scatter and and a scatter	25/09/2016	<u>9.3</u>	CVE-2016-4723
apple iphone_os apple apple_tv	context or cause a denial of service (NULL pointer dereference) via a crafted app. IOAcceleratorFamily in Apple IOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute	25/09/2016	<u>9.3</u> 9.3	CVE-2016-4724
	arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. IOThunderboltFamily in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a			
apple mac_os_x	normalinerournaming in Apple USA before 10.12 another students to elecute a binary code in a privateged context of case a denial of service (memory corruption) via a crafted app. Web/Kit in Apple IOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service	25/09/2016	<u>9.3</u>	CVE-2016-4727
apple safari	(memory corruption) via a crafted web site. a different vulnerability than CVE-2016-4731. WebKit in Apple IOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a	25/09/2016	<u>9.3</u>	CVE-2016-4729
apple safari	denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4733, CVE- 2016-4724, and CVE-2016-4735.	25/09/2016	<u>9.3</u>	CVE-2016-4730
apple safari	WebKit in Apple IOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4729.	25/09/2016	9.3	CVE-2016-4731
apple safari	WebKit in Apple105 before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4735.	25/09/2016	<u>9.3</u>	CVE-2016-4733
apple safari	WebKit in Apple IOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service, lemmony courruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE- 2016-4733, and CVE-2016-4735.	25/09/2016	<u>9.3</u>	CVE-2016-4734
apple safari	Webkit in Apple 105 before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE- 2016-4733, and CVE-2016-4734.	25/09/2016	<u>9.3</u>	CVE-2016-4735
apple mac_os_x	libarchive in Apple OS X before 10.12 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted file.	25/09/2016	<u>9.3</u>	CVE-2016-4736
apple safari	WebKit in Apple IOS before 10, Safari before 10, VdS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. Bibakit in Apple IOS before 10, OS X before 10.12, VdS before 10, and watchOS before 3 allows remote attackers to execute	25/09/2016	<u>9.3</u>	CVE-2016-4737
apple apple_tv	arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	25/09/2016	<u>9.3</u>	CVE-2016-4738
apple iphone_os	S2 Camera in Apple IOS before 10 and OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4750
apple apple_tv	Apple IOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 mishandle signed disk images, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	25/09/2016	<u>9.3</u>	CVE-2016-4753
apple apple_tv	The kernel in Apple OS X before 10.12, tvOS before 10, and watchOS before 3 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	25/09/2016	7.2	CVE-2016-4775
apple apple_tv	The kernel in Apple IOS before 10, OS X before 10.12, VOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service. (invalid pointer dereference) via a crafted app. The kernel in Apple IOS before 10.2 of S before 10.2 and watchOS before 3 allows attackers to execute arbitrary	25/09/2016	<u>9.3</u>	CVE-2016-4777
apple apple_tv	code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4778
dexis imaging_suite	DEXIS Imaging Suite 10 has a hardcoded password for the sa account, which allows remote attackers to obtain administrative access by entering this password in a DEXIS_DATA SQL Server session.	24/09/2016	<u>10.0</u>	CVE-2016-6532
moxa active_opc_server	Unquoted Windows search path vulnerability in Mona Active OPC server before 2.4.19 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDBRVE% directory. ** DISPUTED ** Open Dental I.6.1 and earlier has a hardcoded MySQL root password, which allows remote attackers to obtain	24/09/2016	7.2	CVE-2016-5793
opendental opendental	** DISPUTE ** Open Dental 16.1 and earlier has a hardcoded M/SQL root password, which allows remote attackers to obtain administrative access by leveraging access to instrant CFP one 3306. NOT: the vendor disputes this saw, stating that the *uninerability note is factually failse there is indeed a default blank password, but it can be changed We recommend that users change 1 each customer receives direction.**	24/09/2016	7.5	<u>CVE-2016-6531</u>

Semana 19/09/2016				
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
artifex mupdf	Heap-based buffer overflow in the pdf_load_mesh_params function in pdf/pdf-shade.c in MuPDF allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a large decode array.	22/09/2016	7.5	CVE-2016-6525
cisco - cloud_services_platform_2100	The web-based GUI in Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote authenticated administrators to execute arbitrary OS commands as root via crafted platform commands, aka Bue ID CSCva00541.	22/09/2016	<u>9.0</u>	CVE-2016-6373
cisco - cloud_services_platform_2100	Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote attackers to execute arbitrary code via a crafted dnslookup command in an HTTP request, aka Bug ID CSCuz89093.	22/09/2016	7.5	CVE-2016-6374
cisco - email_security_appliance	Cisco ironPort Async05 9.1.2-023, 9.1.2-028, 9.1.2-036, 9.7.2-046, 9.7.2-047, 9.7.2-054, 10.0.0-124, and 10.0.0-125 on Email Security Appliance (ESA) devices, when Enrollment Client before 1.0.2-065 is installed, allows remote attackers to obtain root access via a connection to the testing/debugging Interface, alsa Bug Dis CSA/DBG7.	22/09/2016	<u>10.0</u>	CVE-2016-6406
cisco – ios	lox in Cisco IOS, possibly 15.6 and earlier, and IOS XE, possibly 3.18 and earlier, allows local users to execute arbitrary IOx Linux commands on the guest OS via crafted lox command-line options, aka Bug ID CSCuz59223.	22/09/2016	7.2	CVE-2016-6414
huawei usg2100_firmware	Buffer overflow in the Authentication, Authorization and Accounting (AAA) module in Huawei USG2100, USG2200, USG5100, and USG5500 unified security gateways with software before V300R001C105PC600 allows remote authenticated RADIUS servers to execute arbitrary code by sending a cartefet APP packet.	22/09/2016	7.1	CVE-2016-6669
lenovo bios	The BIOS for Lencor ThinkCentre E33, M65004; M6600, M6600, M6600, M66004; M730, M880, M85004; M86004; M8600, M M983, and M394 for extension: ThinkServer E4400, RS140, TS140, TS200, TS400, and TS400 devices; and ThinkSation E32, P300, and P310 devices: ThinkServer E4400, RS140, TS140, TS200, TS400, and TS400 devices; and ThinkSation E32, P300, and P310 devices: ThinkServer E4400, RS140, TS140, TS200, TS400, and TS400 devices; and ThinkSation E32, P300, and P310 devices: ThinkServer E4400, RS140, TS140, TS200, TS400, and TS400 devices; and ThinkSation E32, P300, and P310 devices: ThinkServer E4400, RS140, TS140, TS400,	22/09/2016	7.2	<u>CVE-2016-5247</u>
mozilla – firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	22/09/2016	7.5	CVE-2016-5256
mozilla – firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	22/09/2016	<u>7.5</u>	CVE-2016-5257

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
mozilla – firefox	Heap-based buffer overflow in the nsCaseTransformTextBunFactory::TransformString function in Mozilla Firefox before 49.0 and Firefox ISR 45.x before 45.4 allows remote attackers to cause a denal of service (boolean out-of-bounds write) or possibly have unpacefield other impact via Unidoe characters that are unishandled during text conversion.	22/09/2016	7.5	CVE-2016-5270
mozilla – firefox	Use-after-free vulnerability in the nsFrameManager:-CaptureFrameState function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by levenging improper interaction between restyling and the Web Animations model imalementation.	22/09/2016	<u>7.5</u>	CVE-2016-5274
mozilla – firefox	Use-after-free vulnerability in the mozilla::a11y::DocAccessible::ProcessinvalidationList function in Mozilla Firefox before 49.0 and Firefox ESA 45.x before 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corrustion) via an arbi-owns attribute.	22/09/2016	<u>7.5</u>	CVE-2016-5276
mozilla – firefox	Use-after-free vulnerability in the nsRefreshDriver::Tick function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging improper interaction between timeline destruction and the Web Animations model implementation.	22/09/2016	<u>7.5</u>	CVE-2016-5277
mozilla – firefox	Use-after-free vulnerability in the mozilia::nsTextNodeDirectionalityMap::RemoveElementFromMap function in Mozilia Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code via bidirectional text.	22/09/2016	7.5	CVE-2016-5280
mozilla – firefox	Use-after-free vulnerability in the DOMSVGLength class in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between JavaScript code and an SVG document.	22/09/2016	<u>7.5</u>	CVE-2016-5281
redhat quickstart_cloud_installer	Red Hat QuickStart Cloud Installer (QCI) uses world-readable permissions for /etc/qci/answers, which allows local users to obtain the root password for the deployed system by reading the file.	22/09/2016	7.2	CVE-2016-6322
apache – cxf_fediz	the not password for the deployed system by reading the file. The application piperin Fayecher CF field 1.2 x before 1.2 3 and 1.3 x before 1.3.1 do not match SAM. AudienceRestriction values application piperine X and X and SAM. Note with a truncit definition of the system of the s	21/09/2016	<u>7.5</u>	CVE-2016-4464
flex_project flex	Heap-based buffer overflow in the yy_get_next_buffer function in Flex before 2.6.1 might allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via vectors involving num to read.	21/09/2016	7.5	CVE-2016-6354
fortinet fortiwan	Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users with access to the nslookup	21/09/2016	9.0	CVE-2016-4965
huawei ws331a_router_firmware	Eunctionality to execute arbitrary commands with root privileges via the graph parameter to disenosis: control.php. Multiple cross-site request forgery (CSRF) vulnerabilitis in Huawei WS331a routers with software before WS331a-10 V100R00103112 allow remote attackers to hijack the authentication of administrators for requests that [1] restore factory	21/09/2016	7.1	CVE-2016-6158
libarchive libarchive	settings or (2) rebost the device via unspecified vectors. Integer overflow in the ISO9660 writer in ilbarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a	21/09/2016	7.5	CVE-2016-6250
openjpeg openjpeg	Use-after overflow. Use-after-free vulnerability in the opj_j2k_write_mco function in j2k.c in OpenJPEG before 2.1.1 allows remote attackers to have	21/09/2016	7.5	CVE-2015-8871
openjpeg openjpeg xen xen	unspecified impact via unknown vectors. Xen 4.5.3, 4.6.3, and 4.7.x allow local HVM guest OS administrators to overwrite hypervisor memory and consequently gain host	21/09/2016	7.2	CVE-2015-8871
xen xen	OS privileges by leveraging mishandling of instruction pointer truncation during emulation. Use-siter-free vulnershilling in the FFPG event channel code in Ken 4.4. sillows local guest OS administrators to cause a denial of pervice float craft and possibly execute abilityers code or obtain sensible information via an invalid guest frame number.	21/09/2016	<u>72</u> 72	CVE-2016-7093
	service (nost crash) and possibly execute arbitrary code or obtain sensitive information via an invalid guest frame number. Dentsply Sirona (formerly Schick) CDR Dicom 5 and earlier has default passwords for the sa and cdr accounts, which allows	20/09/2016		
dentsply_sirona cdr_dicom	remote attackers to obtain administrative access by leveraging knowledge of these passwords. Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain		<u>10.0</u>	CVE-2016-6530
emc avamar_server	Toot privileges by leveraging admin access and entering a sudo command. The SMB service in EMC VNRe, VNX.F [Ie OE before 7.1.80.3, and VNX2 FIIe OE before 8.1.9.155 does not prevent duplicate	20/09/2016	7.2	CVE-2016-0905
emc vnx1_oe_firmware	NTLM challenge-response nonces, which makes it easier for remote attackers to execute arbitrary code, or read or write to files, via a series of authentication requests, a related issue to CVE-2010-0231.	20/09/2016	<u>7.5</u>	CVE-2016-0917
emc avamar_server	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain root access via a crafted parameter to a command that is available in the sudo configuration.	20/09/2016	7.2	CVE-2016-0920
hp loadrunner	HPE Performance Center before 12.50 and LoadRunner before 12.50 allow remote attackers to cause a denial of service via unspecified vectors.	20/09/2016	<u>9.0</u>	CVE-2016-4384
mariadb mariadb	Oracle MyGQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15, MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17, and Persona Server before 5.5.51.938, 1,5.6.x before 5.6.32.780, and 5.7.x before 5.7.14.7 allow local uses to create arbitrary comparations and sponse screatin protection mechanism by stering general [bg, [Br on any cdf configuration. NOT: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib.	20/09/2016	<u>10.0</u>	CVE-2016-6662
apple xcode	otool in Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4705.	18/09/2016	7.2	CVE-2016-4704
apple xcode	otool in Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4704.	18/09/2016	7.2	CVE-2016-4705
aver eh6108h+_firmware	AVer Information EH6108H+ devices with firmware X9.03.24.00.07I have hardcoded accounts, which allows remote attackers to obtain root access by leveraging knowledge of the credentials and establishing a TELNET session.	18/09/2016	10.0	CVE-2016-6535
aver eh6108h+_firmware	Updation over access or prevent approximiting on the creating and escalarising a restrict session. The /setup URI on AVer Information EH6108H+ devices with firmware \$9.03.24.00.071 allows remote attackers to bypass intended page-access restrictions or modify passwords by leveraging knowledge of a handle parameter value.	18/09/2016	10.0	CVE-2016-6536
cisco - webex meetings server	Cisco WebEx Meetings Server 2.6 allows remote attackers to cause a denial of service (CPU consumption) by repeatedly accessing the account-validation component of an unspecified service. aka Bug ID CSCur92704.	18/09/2016	7.8	CVE-2016-1483
cisco unified computing system	UCS Manager and UCS 6200 Fabric Interconnects in Cisco Unified Computing System (UCS) through 3.0(2d) allow local users to	18/09/2016	7.2	CVE-2016-6402
rockwellautomation rslogix_500_professional_edition	obtain 05 root access via cardred CLI input, aka Bug ID CSCur91263. Bieffer overflow in Rockwell Automation RSagisk Micro Statter Lite, RSLogis Micro Developer, RSLogis 500 Starter Edition, RSLogis 500 Standard Edition, and RSLogis 500 Professional Edition allows remote attackers to execute arbitrary code via a crafted RSS project file.	18/09/2016	9.3	CVE-2016-5814
yokogawa stardom_fcn/fcj	project inits. Yokogawa STABOM FCN/FCJ controller R1.01 through R4.01 does not require authentication for Logic Designer connections, which allows remote attackers to reconfigure the device or cause a denial of service via a (1) stop application program, (2) change value, or (3) modify application command.	18/09/2016	<u>7.5</u>	CVE-2016-4860
cisco webex_meetings_server	Cisco WebEx Meetings Server 2.6 allows remote attackers to execute arbitrary commands by injecting these commands into an	17/09/2016	9.3	CVE-2016-1482
icu_project	application script, als Bug ID CSCv98130. Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through ST.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact	17/09/2016	7.5	CVE-2016-7415
php - php	via a lone locale attine. ext/standard/vz_unerailuter.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a	17/09/2016	<u>7.5</u>	CVE-2016-7411
php php	partially constructed object. Use-alter/free vulnerability in the widay stack, destroy function in ext/wida/widak.c in PMP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wida/Packet XML document that lacks an end stag for a recorder. field element, leading to mihandling in a widar_destrailare call.	17/09/2016	<u>75</u>	CVE-2016-7413
php php	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unpacefield other impact via a cartele PMA archive, related to ext/phar/jut/ca. dets/phar/jo.	17/09/2016	<u>7.5</u>	CVE-2016-7414
php php	ext/pplyspl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via carlied serialized data.	17/09/2016	<u>7.5</u>	CVE-2016-7417
pivotal cloud_foundry_elastic_runtime	Pivotal Cloud Foundry (PCF) Elastic Runtime before 1.6.34 and 1.7.x before 1.7.12 places 169.254.0.0/16 in the all_open Application Security Group, which might allow remote attackers to bypass intended network-connectivity restrictions by leveraning access to the 169.254.169.254 address.	17/09/2016	<u>7.5</u>	CVE-2016-0896
pivotal operations_manager	Pivotal Cloud Foundry (PCF) Ops Manager before 1.6.17 and 1.7.x before 1.7.8, when vCloud or vSphere is used, does not properly enable SSH access for operators, which has unspecified impact and remote attack vectors.	17/09/2016	7.5	CVE-2016-0897
pivotal rabbitmq	property results soft access to operation, and the soft of the sof	17/09/2016	<u>7.8</u>	CVE-2016-0929
adobe acrobat	Adobe Reader and Acobate before 11.0.17, Acrobate and Acrobate Reader DC Clause Leviner, 10006, 20198, and Acrobate and Acrobate Mader DC Continuous before 15.017, 2000 Windows and OS X 1006 watatakens to seconset abstrary code or carace adenual of annota (immony compation) via sumpetified vectors, a different valuesability than OX - 2014; 4130, CV	16/09/2016	10.0	<u>CVE-2016-6937</u>
adobe acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.3038, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVF-20154255.	16/09/2016	<u>10.0</u>	CVE-2016-6938

Semana 12/09/2016				
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
I	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital_editions	via unspecified vectors, a different vulnerability than CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-	16/09/2016	10.0	CVE-2016-4256
	4261. and CVE-2016-4262.			
	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital_editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-	16/09/2016	10.0	CVE-2016-4257
	4261, and CVE-2016-4262.			
	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital_editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4259, CVE-2016-4260, CVE-2016-	16/09/2016	10.0	CVE-2016-4258
	4261, and CVE-2016-4262.			
	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital_editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4260, CVE-2016-	16/09/2016	10.0	CVE-2016-4259
	4261. and CVE-2016-4262. Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4	16/09/2016	10.0	CVE-2016-4260
adobe digital_editions	4261, and CVE-2016-4262.	10/03/2010	10.0	CVE1201014200
	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4	16/09/2016	10.0	CVE-2016-4261
adobe - digital_editions	4260. and CVE-2016-4262.	10/03/2010	10.0	CVC-2010 4201
	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption)			
adobe digital editions	via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-	16/09/2016	10.0	CVE-2016-4262
0 - 2	4260, and CVE-2016-4261.			
	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified	16/09/2016		
adobe digital_editions	vectors.	16/09/2016	<u>10.0</u>	CVE-2016-4263
	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which			
openssl openssl	allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified	16/09/2016	7.5	CVE-2016-2182
	other impact via unknown vectors.			
openssi openssi	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to			
	cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown	16/09/2016	7.5	CVE-2016-6303
	vectors.			
adobe flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS			
	X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	14/09/2016	10.0	CVE-2016-4272
	than CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-			
	6930, CVE-2016-6931, and CVE-2016-6932.			
1	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on			1
adobe flash player	Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	14/09/2016	10.0	CVE-2016-4274
	different vulnerability than CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283,			
	CVE-2016-4284. CVE-2016-4285. CVE-2016-6922. and CVE-2016-6924.			

Primary Vendor Product	Description Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on	Published	CVSS Score	Source & Patch Info
adobe flash_player	Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-427A, CVE-2016-427B, CVE-2016-4283, CVE-2016-428	14/09/2016	10.0	CVE-2016-4275
adobe flash_player	Adobe Taba Physe before 18:00.375 and 19.x through 23.x before 32.00.182 on Windows and 05.X and before 11.202.435 Uhuna allows attaches to execute abritary code or cause a deniel of service (memory corruption) valumperClied vectors, a different valuenability than CVF-2016-4274, CVF-2016-4280, CVF-2016-4281, CVF-2016-4282, CVF-2016-4282, CVF-2016-4282, CVF-2016-4282, CVF-2016-4282, CVF-2016-4282, CVF-2016-4282, CVF-2016-4283, CVF-2016-4281, CVF-2016-4282, CVF-2016-4283, CVF-2016-4281, CVF-2016-4282, CVF-2016-4283, CVF-2016-4283, CVF-2016-4284, CVF-201	14/09/2016	<u>10.0</u>	CVE-2016-4276
adobe flash_player	Use after-free vulnerability in Adobe Flash Player before 18.0.0.373 and 19.4 through 23.8 before 23.0.0.162 on Windows and 05 X and before 11.202.635 on Linux allows attackers to search arbitrary code vul sumpedified vectors, a different vulnerability than CVF-2016-4272, CVF 2016-6921, CVF-2016-6925, CVF-2016-6926, CVF-2016-6927, CVF-2016-6929, CVF-2016 930, CVF-2016-6931, and CVF-2016-6932.	14/09/2016	<u>10.0</u>	CVE-2016-4279
adobe flash_player	Adobe Flash Player before 18.00.375 and 19.x through 23.x before 23.00.162 on Windows and OS X and before 12.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vetors, a different vulnerability than CV-E30164273, CVE-20164275, CVE-20164275, CVE-20164283, CVE-20164283, CVE-20164283	14/09/2016	<u>10.0</u>	CVE-2016-4280
adobe flash_player	CVF-2016-428. CVF-2016-428. CVF-2016-4922, and CVF-2016-4924. Addbe Flash Physic Hebrie 18.0.0378 and 91.5 whrough 23.5 hebre 23.20.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via umpecified vectors, a different videosithight han CVF-2016-4272, CVF-2016-4276, CVF-2016-4278, CVF-2016-4282, CVF-2016-428, CVF-201	14/09/2016	<u>10.0</u>	CVE-2016-4281
adobe flash_player	CVF.2016 4286, CVF.2016.4285, CVF.2016.4282, and CVF.2016.4292, and CVF.2016.4293, CVF.2016,4293, CVF.2016,4293	14/09/2016	<u>10.0</u>	CVE-2016-4282
adobe flash_player	CVF-2016-4284. CVF-2016-4282, CVF-2016-6022, and CVF-2016-6024. Adobe Flash Player before 18.0.0.375 and 19.a through 23.x before 23.0.0.162 on Windows and 05 X and before 11.2.X02.635 on Ultru allows attackers to execute abilitary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVF-2016-4274, CVF-2016-4275, CVF-2016-4726, CVF-2016-4280, CVF-2016-4281, CVF-2016-4282, CVF-2016-4281, CVF-2016-4282, CVF-2016-4280,	14/09/2016	<u>10.0</u>	CVE-2016-4283
adobe flash_player	Addref Table Flager before TBL0.3.175, and 314 through 7.24 before 22.00.1163 on Windows and 05.X and before 11.2.202.623 on Linux allows attackers to security addregs code or cause a before 22.00.1163 on Windows and 05.X and before 11.2.202.623 on different vulnerability than CVF-2016-627X, CVF-2016-4275, CVF-2016-4280, CVF-2016-4281, CVF-2016-4282, CVF-2016-428X, CVF-2016-428X, CVF-2016-692X.	14/09/2016	<u>10.0</u>	CVE-2016-4284
adobe flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4232, (VZ-2016-4232, CVE-2016-4281, CVE-2016-4281, CVE-2016-4282, CVE-2016-4281, CVE-2016-4282, CVE-2016-4281, CVE-2016-4282, CVE-2016-4282, CVE-2016-4282, CVE-2016-4281, CVE-2016-4282, CVE-2016-4281, CVE-2016-4282, CVE-2016-4281, CVE-2016-481, CVE-20	14/09/2016	<u>10.0</u>	CVE-2016-4285
adobe flash_player	CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924. Integer overflow in Adobe Flash Flayer before 18.00.375 and 19.x through 23.x before 23.00.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors.	14/09/2016	<u>10.0</u>	CVE-2016-4287
adobe flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 om Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6923, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6929,	14/09/2016	<u>10.0</u>	CVE-2016-6921
adobe flash_player	(693), CV-2016-6931, and CV-2016-6932. Addee Flash Player before 18.00.375 and 19.a through 23.a before 23.00.162 on Windows and OS X and before 11.2.202.635 on Ultura allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CV-2016-8274, CVE-2016-8275, CVE-2016-4726, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4281, CVE-2016-42	14/09/2016	10.0	CVE-2016-6922
adobe flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.00.375 and 19.x through 23.x before 23.00.160 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability han CVE-2016-4272, CVE-2016-4279, CVE-2016-6925, CVE-2016-6925, CVE-2016-6929, CVE-2016-	14/09/2016	<u>10.0</u>	CVE-2016-6923
adobe flash_player	(#30. CVA. 2016;4911. and CVA. 2016;4912. Addoe Flash Physics Before 113.0.237 explored 39. stmough 23.x before 23.0.0.162 on Windows and CS X and before 11.2.202.635 on Linna allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via umpecified vectors, a different vinterabulty. Into CVX. 2016;472, CVX	14/09/2016	<u>10.0</u>	CVE-2016-6924
adobe flash_player	CVF-2016-4285, CVF-2016-4284, CVF-2016-4284, AVF-2016-4287, and CVF-2016-6927. Use-after-free valueshilly in Addee Hard Hirper before 1840.0375 and 19 x through 23 x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability man CVF-2016-4292, CVF-2016-4272, CVF-2016-4232, CVF-2016-4293, CVF-2016-420, CVF-2016-420	14/09/2016	<u>10.0</u>	CVE-2016-6925
adobe flash_player	4930. CVX-2016-6911. and CVX-2016-6922. Use-after-free vulnerability in Addee Bah Pikere Before 18.00.375 and 19 x through 23 x before 21.0.0.162 on Windows and OS X and before 11.2.202.685 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability and CVX-2016-4927, CVX-2016-4927, CVX-2016-4923, CVX-2016-4923, CVX-2016-4925, CVX-2016-4923, CVX-2016-492, CVX	14/09/2016	<u>10.0</u>	CVE-2016-6926
adobe flash_player	6930, CV-2016-6931, and CV-2016-6932. Use-after-free vulnerability in Addee fields Piliper Before 18.00.375 and 19 x through 23 x before 23.0.0.162 on Windows and OS X and before 11.2.202.685 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability finan CV-2016-4927, CV-2016-492, CV-	14/09/2016	<u>10.0</u>	CVE-2016-6927
adobe flash_player	6930. CVX-2016-6911. and CUX-2016-6912. Use-after-free vulnerability in Addee flash Pilepre Before 18.00.375 and 19 x through 23 x before 23.0.0.162 on Windows and OS X and before 11.2.2016.836 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability finan CVX-2016-4927, CVX-2016-4927, CVX-2016-6923, CVX-2016-6925, CVX-2016-6927, CVX-2016-6927, CVX-2016-6923, CVX-2016-692,	14/09/2016	<u>10.0</u>	CVE-2016-6929
adobe flash_player	6930, CV-3016-6931, and CV-2016-6932. Use-after-free valueshilly in Addee flash Pilyere Before 18.00.375 and 19 x through 23 x before 23.0.0.162 on Windows and OS X and before 11.2.202.685 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability in Addee 10.002 (V-2016-6932, CV-2016-6932,	14/09/2016	<u>10.0</u>	CVE-2016-6930
adobe flash_player	6922, Ork. 2016-6931, and CUF-2016-6932. Use-after-free vulnerability in Addee frain Player Before 18.00.375 and 19 x through 23 x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability frain OVE-2016-4925, OVE-2016-6932, OVE-2016-6932, OVE-2016-6935, OVE-2016-6935, OVE-2016-6935, OVE-2016-6932, OVE-2016-693, OVE-20	14/09/2016	<u>10.0</u>	CVE-2016-6931
adobe flash_player	6922, OCY-2016-6930, and OCY-2016-6932. Use after-free functionality in Adobe Flash Physe before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.653 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than VCF-2016-6922, OCF-2016-6923, OCF-2016-6923, OCF-2016-6925, OCF-2016-6925, OCF-2016-6927, OC-2016-6927, OC-2016-6927, OC-2016-6923, OCF-2016-6923, OCF-2016-6923, OCF-2016-6925, OCF-2016-6927, OC-2016-6925, OCF-2016-6927, OC-2016-6925, OCF-2016-6927, OC-2016-6925, OCF-2016-6925, OCF-2016-692	14/09/2016	<u>10.0</u>	CVE-2016-6932
microsoft edge	1925, VCF2010 9330, and VCF2010 9331. Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVF-2016-3330.	14/09/2016	7.6	CVE-2016-3294
microsoft edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted	14/09/2016	7.6	CVE-2016-3330
microsoft windows_10	web site, alsa "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVF-2016-3294. The SMMV server in Microsoft Windows Vista 5/2, Windows Server 2008 5/2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Cold and R2, Windows R7 8.1, and Windows 10 Cold, S11, and 16/3 Palows remote attackers to execute	14/09/2016	9.0	CVE-2016-3345
	arbitrary code via crafted packets, aka "Windows SMB Authenticated Remote Code Execution Vulnerability." Microsoft Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain			
microsoft windows_10	Microsoft Vensiones zus vala a czałe Odorno, brzyber na proper y mini che permosalne, wmini dłowi naca u deser Urbudan daministrzkar o kaja a czałe Oddi Jala Windows Permosions findercement Elevation of Private Vinerzabilly. <sup>1</sup> The kernel-mode driver sin Microsoft Windows Vita \$92, Windows Server 2008 592 and 82 591, Windows 8.1, Windows Server 2012 Cold and R2, Windows Y 81, and Windows S1 Cold, S11, and 1607 alben colar user to gain privileges via	14/09/2016	7 <u>2</u> 93	CVE-2016-3346 CVE-2016-3348
	a crafted application, aka "Win32k Elevation of Privilege Vulnerability." The kernel-mode drivers in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold			
microsoft windows_10 microsoft edge	and 1511 allow local users to gain privleges via a crafted application, aka "Win32k Elevation of Privlege Vulnerability." The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code crause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," ad ifferent vulnerability	14/09/2016	7.2 7.6	CVE-2016-3349 CVE-2016-3350
microsoft windows 10	than CVE-2016-3377. The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1 windows Server 2012 Gold and R2. Windows RT 8.1. and Windows 10 Gold. 1511. and 1607 allows local users to	14/09/2016	7.2	CVE-2016-3355
microsoft windows 10	gain privileges via a crafted application, aka "GDI Elevation of Privilege Vulnerability." The Graphics Device Interface (GDI) in Microsoft Windows 10 1607 allows remote attackers to execute arbitrary code via a	14/09/2016	9.3	CVE-2016-3356
microsoft office	crafted document. ala "GGI Remote Code Sexuction Vulnerability." Microsoft Office 2007 99, Office 2013 99, Office 2013 99, Office 2013 91, Office 2016, Word for Mac 2011, Word 2016 for Mac, Word Viewer, Word Automation Services on SharePoint Server 2010 92, SharePoint Server 2013 91, Excel Automation Services on SharePoint Server 2013 91, Word Automation Services on SharePoint Server 2013 91, Office Web Apps 2010 92, and Office Web Apps Server 2013 93 91, Word Automation Services on SharePoint Server 2013 91, Office Web Apps 2010 92, and Office Web Apps Server 2013 91, Word Automation Services on SharePoint Server 2013 91, Office Web Apps 2010 92, and Office Web Apps Server 2013 91, Word Automation Services on SharePoint Server 2013 91, Office Web Apps 2010 92,	14/09/2016	<u>93</u>	CVE-2016-3357
microsoft excel	and Office Web Apps Server 3013 397 allow remote stackers to excut a shiftary code via a critical document, also "Microadi Office Memory Control Values and Control Values" (Control Values and Control And Control And Control Values) (Control Values), and and an analysis of the Control Values of the Control Values of the Control Values of the Pack 591, Each Values, Data Services on StarePoint Server 2003 594, Each Services on SharePoint Server 2005 592, Each Automation Services on SharePoint Server 2013 591, and Office Online Server 3100 591, Server 2015 591, and Office Online Server 3100 592, Each Automation Services on SharePoint Server 2013 591, and Office Online Server 3100 592, Each Values of Server 2015 591, and Office Online Server 3100 591, Server 2015 591, and Office Online Server 3100 592, Each Values of Server 2015 591, and Office Online Server 3100 591, and Server 2015 591, and Office Online Server 3100 591, and Server 3100 592, Each Values of Server 2015 591, and Office Online Server 3100 591, and Server 3100 59	14/09/2016	<u>9.3</u>	CVE-2016-3358
microsoft excel	via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute	14/09/2016	9.3	CVE-2016-3359
microsoft office_compatibility_pack	arbitrary code via a crafted document, ala "Microsoft Office Memory Comption Vulnerability." Microsoft Rowerbini 2003 PSP, Rowerbini 2003 PSP, Rowerbini 2013 PSP, NoverPoint 2016 for Mac, Office Compatibility Pack PSP, Rowerbini tt Viewer, SharePoint Server 2013 PS1, Office Web Apps 2010 PS2, and Office Web Apps Server 2013 PS1 allow remote attackers to execute arbitrary code via a crafted document, ala "Microsoft Office Memory	14/09/2016	9.3	CVE-2016-3360
microsoft excel	Corruption Vulnerability." Microsoft Excel 2010 SP2 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	<u>9.3</u>	CVE-2016-3361
microsoft excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Viewer allow remote attackes to execute arbitrary code via a crafted document, Jak Microsoft Office Alemany Compution Viewerbility, a different viewallow than View 5346.	14/09/2016	9.3	CVE-2016-3362
microsoft excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a carleted document, aka "Microsoft Office Memory Corruption Vulnersbilly", Valnersbilly", Valnersbilly,	14/09/2016	<u>9.3</u>	CVE-2016-3363
microsoft visio	Microsoft Visio 2016 allows remote attackers to execute arbitrary code via a crafted document, ala "Microsoft Office Memory Comptition Vulnerality". Microsoft Scal 2007 3PS, Eacel 2013 SP1, Eacel 2013 SP1, Eacel 2013 RT SP1, Eacel 2016, Office Compatibility Pack SP3, Eacel Viewer, Eacel Services on SharePoint Server 2007 SP3, Eacel 2013 RT SP1, Eacel 2016, Office Compatibility Pack SP3, Eacel	14/09/2016	<u>9.3</u> 9.3	CVE-2016-3364
microsoft excel	on SharePoint Server 2013 SPL, and Office Deline Server allow remote attackers to execute arbitrary code via a crafted document, alsa "Microsoft Office Memory Comption Vulnerability," a different vulnerability than CVE-2016-3362. StringBuilder in Microsoft Silverlight 5 before 51.50708.0 does not properly allocate memory for string-insert and string-append operations, which allows remote attackers to execute arbitrary code via a crafted web site, alsa "Microsoft Silverlight Memory	14/09/2016	93	CVE-2016-3365
microsoft silvenight	Operations, Winking allows fremote arcackers to execute arteriary code va a cratter west parts, and "Ancrosoft sinvengent executes arteriary code va a cratter west, and "Ancrosoft sinvengent executors", Microsoft Windows Vista Syra, Windows Server 2008 SP2 and R2 SP1, Windows T Suffyrations as 1, Windows Entrary Code by and R2, Windows R1 8, 1, and Windows Sorts D Codd, S111, and R2 SP1, Windows T Suffyrations are to execute arteriary code by	14/09/2016	9.0	CVE-2016-3368
microsoft windows_10	leveraging a domain account to make a crafted request, aka "Windows Remote Code Execution Vulnerability." Microsoft Windows 10 Gold and 1511 allows attackers to cause a denial of service via unspecified vectors, aka "Windows Denial	14/09/2016	<u>7.8</u>	CVE-2016-3369
microsoft internet_explorer	of Service Vuberzebilty." The OLL Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, Windows Vita SP2, Windows Server 2008 SP2 and R2 SP1, Windows 751, Windows 8.1, Windows Server 2012 Cold and R2, Windows R1 8.1, and Windows 10 Cold, 151, and 1627 Jahren wentee attackers to secure abritary cold or crusse a denial of service (memory	14/09/2016	7.6	CVE-2016-3375
microsoft edge	comption) via a carlied web site, alsa "Soripting Engine Memory Comption Vulnerability." The Chakra Jacobige engine in Microsoft Edge allows removed tatkkens to execute sehtrary concerning a denial of anrice thermony comption) via a carlied web site, alsa "Soripting Engine Memory Comption Vulnerability," a different vulnerability than CVF 2015 and the set of	14/09/2016	7.6	CVE-2016-3377
L	than CVE/2010/5550.	I	I	1

Printery Visioder - Brooket         Description           microsoft	"Microard Diffes Memory Computer ison Control Trighter generation SSL or (2) 11.5 packets, alsa Bing (2) Eastern to cause a denial of service (device movies) and the service (device movies) in Androad back 2016; 400 cost inter provides a long string, alsa Android Calcido Adu, and 20 before 2016; 400 cost inter provides a long string, alsa Android Calcido Adu, al size and a string string and the service of the service of the service of the service of the service of the service of the service of the service of the service of the calcido Adu, al size and the service and the service of th	Published 14/09/2016 12/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	23 24 24 23 23 23 23 23 23 23 23 23 23 23 23 23	Source & Patch Info Orf. 2016 3133 Crif. 2016 4132 Crif. 2016 4132 Crif. 2016 4152 Crif. 2016 3152 Crif. 2016 3152 Crif. 2016 3155 Crif. 2016 3155 Crif. 2016 3155 Crif. 2016 3155 Crif. 2016 3155 Crif. 2016 3155
microaff         Veew allow more attracts to excert a bitrary code via a carted document, application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         Class AEEE Application Control Tuple Modular through AS 120-18.0.           consolid         AEEE Transmission Control Tuple Modular through AS 120-18.0.           progle - android         AEEE Transmission Control Tuple Modular through AS 120-18.0.           progle - android         The Claskomm comers diver in Android thron 200-050-050 on Neurs 5, Neuro 5, SU, and the Class AS 120-18.0.           progle - android         The Claskomm comers diver in Android thron 200-050 on Neurs 5, Neuro 5, SU, and the Class AS 120-18.0.           progle - android         The Claskomm comers diver in Android thron 200-050 on Neurs 5, Neuro 4, AS 10.           progle - android         The Claskomm relation through application, and android thron 201-050 on Neuro 5, Neuro 4, Neuro 4, AS 10.           progle - android         The Claskomm Neuro Modular through application, and android through applicalin, and android through ap	"Microard Diffes Memory Computer ison Control Trighter generation SSL or (2) 11.5 packets, alsa Bing (2) Eastern to cause a denial of service (device movies) and the service (device movies) in Androad back 2016; 400 cost inter provides a long string, alsa Android Calcido Adu, and 20 before 2016; 400 cost inter provides a long string, alsa Android Calcido Adu, al size and a string string and the service of the service of the service of the service of the service of the service of the service of the service of the service of the calcido Adu, al size and the service and the service of th	12/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	7.8           9.3	CH-2016-6329 CH-2016-1829 CH-2016-1829 CH-2016-1829 CH-2016-1859 CH-2016-1859 CH-2016-1859 CH-2016-1855 CH-2016-1855 CH-2016-1855 CH-2016-1855
exc =	551 or (2) TLS packets, aka Bug ID tackets to cours a denial of service (device) me over in Advord beine 22166 49 cost and the to course a denial of service (device) me over in Advord beine 22166 49 cost at provides a long string, aka Advord Devices allower string, aka Advord Devices allower string, aka Advord Cost 400, una r 2 of beine 2016 40- en string the string and the service and the service and the string term of the service and the service and the service allower remote a string the service and the service and the service and the service and the allower string term of the service allower string terms beine string term of the service and the service allower string terms beine string terms of the service string terms of the service string terms of the service string terms of the service string terms beine string terms of the service string terms of the service string terms beine string terms of the service string terms of the service string terms beine string terms of the service	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	2.8         9.3           9.3         9.3           9.3         9.3           9.3         9.3           9.3         9.3           9.3         9.3           9.3         9.3           9.3         9.3	CH-2016-1859 CH-2016-1859 CH-2016-1859 CH-2016-1852 CH-2016-1854 CH-2016-1854 CH-2016-1854 CH-2016-1856 CH-2016-1856 CH-2016-1856
Bund * genologie android         Bedard via survival         Bedard via survival           Bigle - android         Bigle - bendraid in the survival surv	m driver in Android before 2016 69 05 on the provides a long string, als Android 2016 69 01, and 5 02 000 000 box 2016 69 01, and 5 02 000 000 m within, which allows remote attacken to carable flux, alterest to again privileges to again the string of the	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	93 93 93 93 93 93 93 93 93 93 93	CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3855 CH-2016-3857
page - android heads SX and GP device site attacks to get in page sets attack to get approxement of the page of the sets of t	het providers allows attrackers to gain privileger and an experimental statistics to gain privileger and an experimental statistics of gain privileger and an experimental statistics of gain privileger and an experimental statistics of the and and and and privileger and an experimental statistics of the analysis of the constraints of the analysis of the analysis of the analysis of the constraints of the analysis of the analysis of the own attackers to gain privileges the analysis of the analysis of the own attackers to gain privileges the analysis of the analysis of the other of the advector	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	93 93 93 93 93 93 93 93 93 93	C/F-2016-3852 C/F-2016-3852 C/F-2016-3854 C/F-2016-3854 C/F-2016-3856 C/F-2016-3856 C/F-2016-3856 C/F-2016-3856
pipels – android         The Quakemm camera driver in Android beform 2016-09 Go mesos, S, SK, and Bellow, SM, SK, and SK, SK, SK, and SK, SK, SK, and SK,	bug CR10144.1 Disc CR10144.1 Disc O+0.1, and 7.0 before 2016-09-01 Disc O+0.1, and 7.0 before 2016-09-01 Disc O+0.1, and 7.0 before 2016-09- out and the physical behavior and the physical 2.5.1.1 before 5.1.1, and 6.1 before 2016-09- our remote attackers to concute arbitrary remain bag 20270460. Si, Neuro F, Reuss GF, and Andreid Ohe and Bag 20232734 and Gaukcomm Internal Protes allows attackers to gain privileges via a 2010/2007 before 5.0.2, and the physical before 2010/2007 before 5.0.2, before 2010/2007 before 5.0.2, bit before Changes, which allows attackers to gain privileges via a 2010/2007 before 5.0.2, bit before Changes, which allows attackers to gain privileges via a caffed was attackers to gain privileges via a 2010/2007 before 5.0.2, bit before changes, which allows attackers to gain was attackers to gain was a caffed was attackers to gain privileges via a 2010/2007 before 5.0.2, bit before changes, which allows attackers to gain was attackers to gain privileges via a constant of the source of the source of the source of the dist of the source of the source of the source of the dist of the source of the source of the source of the dist of the source of the source of the source of the dist of the source of the source of the source of the dist of the source of the source of the source of the dist of the source of the source of the source of the source of the dist of the source of the dist of the source of the sourc	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	93 93 93 93 93 93 93 93 93	CVF-2016-3861 CVF-2016-3862 CVF-2016-3864 CVF-2016-3865 CVF-2016-3865 CVF-2016-3865 CVF-2016-3867
peogle – android excitational and an excitation of the excitation	ng widths, wich allows remote attacken to crafted file, all internal bag 3220543. 2, 5, 1, 1 before 5, 1, 1, and 6 a before 2016 GP some remote attacken to benecite attacken all log 282027046. 2, 5, 1, 2 before 5, 1, 2, and 6 a before 2016 GP some remote attacken to gain privileges via a 2010/2021 A and Qualcomm internal invice allows attacken to gain privileges via a 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges via 2010/2021 A some of the some remote attacken to gain privileges attacken to gain privileges via a 2010/2021 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the 2010 A some of the some of the some of the some of the some of the 2010 A some of the some of the some of the some of the some of the 2010 A some of the some of the some of the some of the some of the 2010 A some of the some of the some of the some of the some of the 2010 A some of the some of	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	93 93 93 93 93 93 93	CVF-2016-3862 CVF-2016-3864 CVF-2016-3865 CVF-2016-3865 CVF-2016-3865 CVF-2016-3865
people – android         Di doos not propriy interact with the used function statistics in the people without	own remote attackers to execute arbitrary error bage 3227044 353, Neura A, Kenuc GP, and Android On- al bug 2822174 and Qualcomm Internati- netices allows attackers to gain privileges via a 201203202 20120320, and attackers to gain privileges via a 20120320, and attackers to gain privileges via a 20120320, Amount Payer, and Paice 20120320, Amount Payer, and Paice 20120320, Amount Payer, and Paice 20120320, and attackers to gain privileges via a 20120327, and and attackers to gain privileges via a 20120327, and attackers to gain privileges via a cathed distackers to gain privileges via a cathed	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	9 <u>3</u> 9 <u>3</u> 9 <u>3</u> 9 <u>3</u> 9 <u>3</u>	CVE-2016-3864 CVE-2016-3865 CVE-2016-3866 CVE-2016-3867
people - android devices allows attackens to gain privately va a called application, also Android terms backet 201117. prople - android The Synaptics Exclusion and an entry that 2209226. prople - android The Synaptics Exclusion and an entry that 2209226. prople - android The Synaptics Exclusion and an entry that 2209226. prople - android The Synaptics Exclusion and an entry that 2209226. prople - android The Quadration also Android Internal bac 2016056 on Neuros S1 and 09 does the Synaptics Exclusion and an entry that 2018056. prople - android The Quadration also Android Internal bac 2018056 and Quadration Internal back 2018056 and Quadration Internal back 2018056 and Quadration Neurol Internal Back 2018056 and Quadration Internal back 2018056 and Quadratic Android Interna Back 2018056 and Quadratic Android Internal Back 2018056 and Quadratic Android Interna Back 2018056 and Quadratic Android Internal Back 2018056 and Quadratic Andr	val log 28822734 and Qualcomm Internal moleculations attackers to gain privileges via a valence allow attackers to gain privileges via a 281037807 281037807 281037807 48104 To gain privileges via a 281037807 481, heaves Hoyer, and Hort Call 181037807 481, heaves Hoyer, and Hort Call 181027097 481, heaves Hoyer, and Hort Call 181027097 18104 To gain privileges via a 28103787 28103787 481, heaves Hoyer, and Hort Call 181047 1	11/09/2016 11/09/2016 11/09/2016 11/09/2016 11/09/2016	9.3 9.3 9.3 9.3	CVE-2016-3865 CVE-2016-3866 CVE-2016-3867
jangler - android  projekt - and	vices allows attackers to gain privileges via a 2010/2000 or to gain privileges via a 2010/2000 gain privileges via a 2010/2000 gain gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain gain 2010/2000 gain gain gain gain gain gain gain 2010/2010 gain gain gain gain gain gain gain gain	11/09/2016 11/09/2016 11/09/2016 11/09/2016	93 93 93	CVE-2016-3866 CVE-2016-3867
proger – android proge	TRIDIZED OFFICIENT OF SHIP STUDIES AND	11/09/2016 11/09/2016 11/09/2016	<u>9.3</u> <u>9.3</u>	CVE-2016-3867
grage - android         The Quakerami NP & driver in Android Deriver 2016-09 G is in Neural Stard of Policess cardina application, advanciationisma bug 2019ability and Quakeraminema bug 1 (Progle - android)           The Quakerami NP and Policy 2016-09 G is in Neural Stard of Policess (Progle - android)         The Quakerami NP and Policy 2016-09 G is Neural Stard of Policess (Progle - android)           The Dukerami NP and Policy 2016-09 G is Neural Stard of Policess (Progle - android)         The Dukerami NP android Stard Policess (Progle - android)           grage - android         The Dukerami NP android Stard Policy 2016-09 G is Neural Stard (Progle - android)         Neural Stard Policy 2016-09 G is Neural Stard Policy 2016-09 G is Neural Stard (Progle - android)         Neural Stard Policy 2016-09 G is Neural Stard (Progle Neural Stard)           grage - android         1.1.1.4. Is Netro 2016-09 G is Neural Stard (Progle Neural Stard)         Neural Stard (Progle Neural Stard)           grage - android         1.1.1.4. Is Netro 2016-09 G is Neural Stard (Progle Neural Stard)         Neural Stard (Progle Neural Stard)           grage - android         1.1.1.4. Is Netro 2016-09 G is neural Stard (Progle Neural Stard)         Neural Stard (Progle Neural Stard)           grage - android         1.1.1.4. Neural Neural Neural Neural Neural Neural Stard (Progle Neural Stard)         Neural N	allows attackers to gain privileges via a F20029997. F20029997. F2002997. F20029787. F20029787. F2002978.	11/09/2016 11/09/2016	9.3	
pogle – android The Quakcomm power driver in Addroid before 3016-096 on Netwos 154 and 0 Percent cardinal administra in Advanced internal base 2016-096 con Netwos 154 and 0 Parlor The Broadcom NH r divers in Advanced before 2016-096 con Netwos 154 and 0 Parlor base 2019 con 2019	es allows attackers to gain privileges via a 20102875. GP, Nexus 9, Nexus Player, and Pixel C and bug 20090925 and Broadcom internal and bug 20090925 and Broadcom internal before 4.4.4, 5.0.x before 5.0.2, 5.1.x before changes, which allows attackers to gain erver in Android 4.A. before 4.4.4, 5.0.x wattackers to gain privileges via a crafted attacker 5.0.2, 6.0.x before 5.0.2.	11/09/2016		CVE-2016-3868
The Backbarn Wit Adverse in Advert Adverse in Advertised Adverse in Adverse in Advertised Adverse in	GP, Nexus 9, Nexus Player, and Pixel C nal bug 29009982 and Broadcom internal before 4.4.4, 5.0.x before 5.0.2, 5.1.x before changes, which allows attackers to gain erver in Android 4.x before 4.4.4, 5.0.x wa ttackers to gain privileges via a crafted indroid 4.x before 4.4.4, 5.0.x before 5.0.2,	11/09/2016		
peogle – andosi devices allows attackens to gin private via a cathod application, as Andord intern the Bieldwinn Bield	nal bug 29009982 and Broadcom internal vefore 4.4, 5.0. before 5.0.2, 5.1.x before changes, which allows attackers to gain erver in Android 4.x before 4.4.4, 5.0.x wa ttackers to gain privileges via a crafted indroid 4.x before 4.4.4, 5.0.x before 5.0.2,		<u>9.3</u>	
people – android  1.1.1, 4, 6 kefers 2016 0F 03, and 7, 2 before 7216 0F 03 been not provent important orthologies - android  2016 0F 03 been not provent important people – android  2016 0F 03 been not provent important important important important 2016 0F 03 been not provent important importan	changes, which allows attackers to gain erver in Android 4.x before 4.4.4, 5.0.x ow attackers to gain privileges via a crafted idroid 4.x before 4.4.4, 5.0.x before 5.0.2,	11/09/2016		CVE-2016-3869
peogle – andosi before 5.0.2, 5.1.3, fee before 2016; 6.9.0, and 7.0 before 2016; 6.9.0, and 2.0.0, and 2.0 before 2016; 6.9.0, and 2.0 befo	ow attackers to gain privileges via a crafted advised of the second seco		<u>9.3</u>	CVE-2016-3870
progle – android	Idroid 4.x before 4.4.4, 5.0.x before 5.0.2,	11/09/2016	<u>9.3</u>	CVE-2016-3871
groge – android     control by 2018497     control by 201849     control by 20184     contr		11/09/2016	<u>9.3</u>	CVE-2016-3872
progle – android properly visited the agriments array, which allows attacks to begin privileges via a WE_UUMT_TST_OUCOMMAN, a knowledge interpret and the 2004/64/20 and Qualcomm progle – android which allows physically provide the 2004/64/20 and 2004 begin progle – android which allows physically provide the 2004/64/20 and 2004 begin progle – android and and and and and and and and and an	to gain privileges via a crafted application,	11/09/2016	9.3	CVE-2016-3873
google – android which allways physically proximites attackers to bypass intended access restrictions and alka internal bug 2651884. provider systemic posterings/bettings/bottings/provider.java in Android 6.x before 2016/09-01 and 7.0 be attackers to bypass the SAFE_000T_DGALLOWED protection mechanism and boot to fabb tool, aka internal bug 29800386.	crafted application that sends a internal bug CR997797.	11/09/2016	<u>9.3</u>	CVE-2016-3874
google – android attackers to bypass the SAFE_BOOT_DISALLOWED protection mechanism and boot to (adb) tool, aka internal bug 29900345.	d boot to safe mode via unspecified vectors,	11/09/2016	<u>7.2</u>	CVE-2016-3875
	o safe mode via the Android Debug Bridge	11/09/2016	7.2	CVE-2016-3876
google – android Unspecified vulnerability in Android before 2016-09-01 has unknown impact and atta		11/09/2016	10.0	CVE-2016-3877
google – android decoder/lh264d_api.c in mediaserver in Android 6.x before 2016-09-01 mishandles th remote attackers to cause a denial of service (device hang or reboot) via a crafted me	edia file, aka internal bug 29493002.	11/09/2016	<u>7.1</u>	CVE-2016-3878
arm-ve-122/klb_srr(ess_mdisc.in mediasener in Android 4.x before 4.4.4, 5.0.x befor 2016-09-01 allows remote attackers to cause a denial of service (NULL pointer derefe crafted media file, aka internal bug 29770686	rence, and device hang or reboot) via a	11/09/2016	7.1	CVE-2016-3879
Multiple buffer overflows in rtsp/AdessionDescription.cpp in libitager[ight in medias before 5.0.2, 5.1.x before 5.1.1, 6.x before 5.016.09.01, and 7.0 before 2016-09.01 is privice i device hanc or reboot i via a crafted media file. aka internal but 25747570.	erver in Android 4.x before 4.4.4, 5.0.x ow remote attackers to cause a denial of	11/09/2016	7.1	CVE-2016-3880
The decoder _peek_si_internal function in vp9/vp9_dx_iface. In iboyo im mediaterov 5.0.2, 5.1. before 5.1.1, 6.1 before 5.10.1, 6.1 before 5.10.16-00.1 allows ren (buffer over-read, and device hang or reboot) via a crafted media file, aka internal bu	note attackers to cause a denial of service g 30013856.	11/09/2016	<u>7.1</u>	CVE-2016-3881
debuggerd/debuggerd.cpp in Debuggerd in Android 5.0.x before 5.0.2, 5.1.x before 5 google – android 2016/99-01 instandes the interaction between PTRACE_ATTACH operations and the privileges via a caffed application, akai Internal bug 295556.	ead exits, which allows attackers to gain	11/09/2016	<u>9.3</u>	CVE-2016-3885
systemu/statusbar/phone/QuickStatusBarHeader.java in the System UI Tuner in And poogle – android prevent tuner changes on the lockscreen, which allows physically proximate attacker alsa interad bug 30107438.	s to gain privileges by modifying a setting,	11/09/2016	7.2	CVE-2016-3886
Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows physically proximate google – android Protection protection mechanism by accessing [1] an external life from a system appl Setting application during a pre-setup stage, also internal bug 29194585.	lication, (2) the help feature, or (3) the	11/09/2016	<u>7.2</u>	CVE-2016-3889
The Java Debug Wire Protocol (JDWP) implementation in add/sockets.cop in Android before 5.1.1, and 6.x before 2016-09-01 mishandles socket close operations, which al application, aka internal bug 28347842.	lows attackers to gain privileges via a crafted	11/09/2016	<u>7.6</u>	CVE-2016-3890
OMXCcodec.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x befor google – android 09-01, and 7.0 before 2016-09-01 does not validate a certain pointer, which allows re (device hang or reboot) via a crafted media file, aka internal bug 29421811.	mote attackers to cause a denial of service	11/09/2016	<u>7.1</u>	CVE-2016-3899
google – chrome Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windo Linux allow attackers to cause a denial of service or possibly have other impact via un	ws and OS X and before 53.0.2785.92 on known vectors.	11/09/2016	7.5	CVE-2016-5167
ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandle php – php remote attackers to cause a denial of service or possibly have unspecified other impa (1) destruct call or (2) magic method call.	s certain invalid objects, which allows	11/09/2016	<u>7.5</u>	CVE-2016-7124
The imagerurecolorbajatte function in ext/gd/gd.c in PHP before 5.6.25 and 7.x bef php – php number of colors, which allows remote attackers to cause a denial of service (select write) or possibly have unspecified other impact via a large value in the third argument	colors allocation error and out-of-bounds	11/09/2016	7.5	CVE-2016-7126
write) or possibly have unspecified other impact via a large value in the third argume The imagenamacorrect function in ex/g/g/g/ i.e. INPP heters 6.2 S2 and 7.2 heters php – php values, which allows remote attackers to cause a denial of service (out-of-bounds wr impact by providing different signs for the second and third arguments.	7.0.10 does not properly validate gamma	11/09/2016	<u>7.5</u>	CVE-2016-7127
The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and php - php cause a denial of service (segmentation fault) or possibly have unspecified other imp demonstrated by a wddx_deematic call that mithandles a dateTime betwenn in a w	7 x before 7.0.10 allows remote attackers to	11/09/2016	<u>7.5</u>	CVE-2016-7129
ext/curl/Interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer or php – php cause a denial of service (allocation error and heap-based buffer overflow) or possible string inth is michanded in a curl escape call.	act via an invalid ISO 8601 time value, as		1	

	Semana 05/09/2016			
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
fortinet fortiswitch	Fertimet FortSwitch FSW 1080-POE, FSW 1240, FSW 1240-POE, FSW 2240-POE, FSW 2240-POE, FSW 2240-POE, FSW 2440-POE,	09/09/2016	<u>10.0</u>	<u>CVE-2016-4573</u>
juniper junos	Juniper Junios OS before 12.1046-045, 12.1046-045, 12.1047 before 12.1047-055, 12.2048 before 12.2048-0409, 13.3 before 13.38495, 14, 14, 1640ere 14.187, 14, 24 foreire 12.3845, 154, 154 before 15.11454, 154 Junie 15.18743, 154 before 15.1874, 354 before 15.1874, 35	09/09/2016	<u>7.8</u>	CVE-2016-1263
juniper junos	Juniper Junos OS Before 12.1346-050, 12.1347 Before 12.1347-040, 12.3348 Before 12.3348-030, 13.3 Before 13.388, 14.1 Before 14.184, 14.1135 Before 14.3353-040, 14.2 Before 13.4286, 15.1 Before 15.1676 or 15.184, 36.1 SLAP6 Defor when configured with a GRE or IPIP funnel, allow remote attackers to cause a denial of service (kernel panic) via a crafted ICMP packet.	09/09/2016	7.1	CVE-2016-1277
juniper junos	J-Web in Juniper Junos 05 before 12.13x6-045, 12.13x6-050, 12.13x7 before 12.13x7-055, 12.3 before 12.3812, 12.3x88 before 12.3x84.052, 13.3 before 13.3810, 13.389 before 13.3895, 13.4 before 14.187, J4.1353 before 14.1353, 055, J4.2 before 14.23x8, 51.5 before 15.13x0 r 51.141, 42.13x8 before 13.13x80, and 51.5 Before 15.188 might allow remote attackes to obtain sensitive information and consequently gain administrative privileges via unspecified vectors.	09/09/2016	<u>10.0</u>	<u>CVE-2016-1279</u>
hp integrated_lights-out_3_firmware	Multiple unspecified vulnerabilities in HPE Integrated Light-Out 3 (aka ILO 3) firmware before 1.88, Integrated Lights-Out 4 (aka ILO 4) firmware before 2.42 allow remote attackers to obtain sensitive information, modify data or cause a denial of service via sunknown vector.	08/09/2016	<u>7.5</u>	CVE-2016-4375
cracklib_project cracklib	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause a denial of service (application crash) or gain privileges via a long GECOS field, involving longbuffer.	07/09/2016	7.2	CVE-2016-6318
f5 – big-ip_access_policy_manager	F 8 100-1P TLA, Analytics, APMA, AMM, and Link Controller 11.2.1. before 11.2.1. before 11.3.4. PLAS, 11.3.5. before 11.3.4. PLAS, 11.5. before 11.5. PLAS, 11.5. be	07/09/2016	7.5	<u>CVF-2016-5022</u>
huawei honor_4c_firmware	The Camera driver in Huave Hinone 4C smartphones with software CMM-ULD0C0D before CMM-ULD0C0DB54A, editM-100C0D before CMM-T0001854A, and CMM-100C0D before CMM-T000C008564 and CMM usus advantative to cause advanial d service crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6183, CVE-2016-6183, and CVE-2016-6184.	07/09/2016	<u>9.3</u>	CVE-2016-6182
huawei uma	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE-2016-7110.	07/09/2016	10.0	CVE-2016-7109
huawei uma	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE-2016-7109.	07/09/2016	10.0	CVE-2016-7110
qemu qemu	The esg. do. dma function in hw/scs/esg.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or execute arbitrary code on the QEMU host via vectors involving DMA read into ESP command buffer.	07/09/2016	7.2	CVE-2016-6351
siemens en100 ethernet module firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic.	05/09/2016	10.0	CVE-2016-7112
siemens en100 ethernet module firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets.	05/09/2016	7.8	CVE-2016-7113
siemens en100_ethernet_module_firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic during an authenticated session.	05/09/2016	9.0	CVE-2016-7114
cisco – webex_wrf_player_t29	Cisco WebEx Meetings Player T29.10, when WRF file support is enabled, allows remote attackers to execute arbitrary code via a crafted file, aka Bug ID CSCva09375.	03/09/2016	<u>9.3</u>	CVE-2016-1464
misp-project malware_information_sharing_platform	app/Controller/Templates/Controller.php in Malware Information Sharing Platform (MISP) before 2.3.92 does not properly restrict filenames under the tmp/files/ directory, which has unspecified impact and attack vectors.	03/09/2016	<u>10.0</u>	CVE-2015-5719
misp-project malware_information_sharing_platform	Malware information Sharing Platform (MISP) before 2.3.90 allows remote attackers to conduct PHP object injection attacks via crafted serialized data, related to TemplatesController.php and populate_event_from_template_attributes.ctp.	03/09/2016	<u>7.5</u>	CVE-2015-5721