Semana 28/11/2016

Primary Vandor Product	Semana 28/11/2016	Published	CVSS Score	Source & Datch Info
Primary Vendor Product	Description In BMC Patrol before 9.13.10.02, the binary "listguests64" is configured with the setuid bit. However, when executing it, it will look for	Published	CVSS Score	Source & Patch Into
bmc patrol	a binary named "virsh" using the PATH environment variable. The "listguests64" program will then run "virsh" using root privileges. This allows local users to elevate their privileges to root.	02/12/2016	<u>7.2</u>	CVE-2016-9638
ibm tivoli_monitoring	Stack-based buffer overflow in the ax Shared Libraries in the Agent in IBM Tivoli Monitoring (ITM) 6.2.2 before FP9, 6.2.3 before FP5, and 6.3.0 before FP2 on Linux and UNIX allows local users to gain privileges via unspecified vectors.	01/12/2016	7.2	CVE-2016-2946
ibm qradar_security_information_and_event_m	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 executes unspecified processes at an incorrect privilege level, which makes it easier for remote authenticated users to obtain root access by leveraging a command-injection issue.	30/11/2016	<u>8.5</u>	CVE-2016-2876
anager dell idrac7_firmware	Dell iDRAC7 and iDRAC8 devices with firmware before 2.40.40.40 allow authenticated users to gain Bash shell access through a string injection.	29/11/2016	9.0	CVE-2016-5685
exponentcms exponent_cms	In framework/modules/core/controllers/expCommentController.php of Exponent CMS 2.4.0, content_id input is passed into showComments. The method showComments is defined in the expCommentControllercontroller with the parameter 'Sthis-	29/11/2016	<u>7.5</u>	CVE-2016-9481
	Sparams['content id']' used directly in SQL. Impact is a SQL injection. The nginx package before 1.6.2-5+deb8u3 on Debian jessie and the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS,			
nginx nginx	before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10 allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.	29/11/2016	7.2	CVE-2016-1247
canonical – ubuntu_linux	The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a	27/11/2016	7.2	CVE-2015-1328
linux linux kernel	configuration in which overlayfs is permitted in an arbitrary mount namespace. The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the	27/11/2016		CVE-2016-8632
iinux iinux_kernei	minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heap- based buffer overflow) by leveraging the CAP NET. ADMIN capability. drivers/vfio/pcit/vfio_pcit.in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial	27/11/2016	7.2	CVE-2016-8632
linux linux_kernel	of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO DEVICE SET IRQS loctl call, aka a "state machine confusion bug."	27/11/2016	<u>7.2</u>	CVE-2016-9083
linux linux_kernel	security/keys/big_key.c in the Linux kernel before 4.8.7 mishandles unsuccessful crypto registration in conjunction with successful key- type registration, which allows local users to cause a denial of service (NULL pointer dereference and panic) or possibly have	27/11/2016	9.3	CVE-2016-9313
	unspecified other impact via a crafted application that uses the big_key data type. The sctp_sf_ooth function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk,			
linux linux_kernel	which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.	27/11/2016	10.0	CVE-2016-9555
linux linux_kernel	Theget_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel 4.4.22 through 4.4.28 contains extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a	27/11/2016	9.3	CVE-2016-9644
	crafted application. NOTE: this vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels. An elevation of privilege vulnerability in libzipfile in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable a			
google android	local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android	25/11/2016	9.3	CVE-2016-6700
	An elevation of privilege vulnerability in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-			
google android	11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-30229821.	25/11/2016	9.3	CVE-2016-6704
	An elevation of privilege vulnerability in Mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This			
google android	nerore 2016-11-01 count enable a local maticipus application to execute arbitrary code within the context or a privileged process. Inits issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-30907212.	25/11/2016	9.3	CVE-2016-6705
google android	An elevation of privilege vulnerability in System Server in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it	25/11/2016	9.3	CVE-2016-6707
google and ou	could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A- 31350622. A remote denial of service vulnerability in Mediaserver in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable an	23/11/2010		<u> </u>
google android	attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30822755.	25/11/2016	7.1	CVE-2016-6713
google android	A remote denial of service vulnerability in Mediaserver in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote	25/11/2016	7.1	CVE-2016-6714
	denial of service. Android ID: A-31092462. An elevation of privilege vulnerability in Mediaserver in Android 4x before 4.4.4, 5.0x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-			
google android	11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Moderate because it first requires exploitation of a separate vulnerability. Android ID: A-31350239.	25/11/2016	7.6	CVE-2016-6717
google android	A denial of service vulnerability in the Input Manager Service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to cause the device to continually reboot.	25/11/2016	7.1	CVE-2016-6724
	This issue is rated as Moderate because it is a temporary denial of service that requires a factory reset to fix. Android ID: A-30568284.		_	,
google android	A remote code execution vulnerability in the Qualcomm crypto driver in Android before 2016-11-05 could enable a remote attacker to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of remote code execution in the context of the kernel. Android ID: A-30515053. References: Qualcomm QC-CREJ050970.	25/11/2016	10.0	CVE-2016-6725
	An elevation of privilege vulnerability in the kernel ION subsystem in Android before 2016-11-05 could enable a local malicious			
google android	application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30400942.	25/11/2016	9.3	CVE-2016-6728
google android	An elevation of privilege vulnerability in the Qualcomm bootloader in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local	25/11/2016	9.3	CVE-2016-6729
	permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30977990. References: Qualcomm QC-CR8977684. An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application.	, , ,	_	
google android	to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30904789. References:	25/11/2016	9.3	CVE-2016-6730
	NVIDIA N-CVF-2016-6730. An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent			
google android	to execute arbitrary cope within the context of the kernel. Into source is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906023. References: NVIDIA N-CVE-2016-6731.	25/11/2016	9.3	CVE-2016-6731
google android	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent	25/11/2016	9.3	CVE-2016-6732
00	device compromise, which may require reflashing the operating system to repair the device. Android ID: A:30906599. References: NVIDIA N-CVE-2016-6732. An elevation of privilese vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application.			
google android	to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906694. References:	25/11/2016	9.3	CVE-2016-6733
	NVIDIA N-CVE-2016-6733. An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application			
google android	to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30907120. References: NVIDIA N-CVE-2016-6734.	25/11/2016	9.3	CVE-2016-6734
google android	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent	25/11/2016	9.3	CVE-2016-6735
00	device compromise, which may require reflashing the operating system to repair the device. Android ID: A:30907701. References: NVIDIA N-CVE-2016-6735. An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application.			
google android	to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30953284. References:	25/11/2016	9.3	CVE-2016-6736
	NVIDIA N-CVE-2016-6736. An elevation of privilege vulnerability in the kernel ION subsystem in Android before 2016-11-05 could enable a local malicious			
google android	application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30928456.	25/11/2016	9.3	CVE-2016-6737
google android	An elevation of privilege vulnerability in the Qualcomm crypto engine driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires	25/11/2016	9.3	CVF-2016-6738
00	compromising a privileged process. Android ID: A-30034511. References: Qualcomm QC-CR#1050538.			
google android	An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernet. This issue is rated as High because it first requires compromising a privileged rungers, android IV—3-00704605, References, Outstromm OF-CRB1099256.	25/11/2016	9.3	CVE-2016-6739
	a privileged process. Android ID: Ar-300/4005. References: Qualcomm QC-CRR1045620. An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious			
google android	application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30143904. References: Qualcomm QC-CR#1056307.	25/11/2016	9.3	CVE-2016-6740
google android	An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious	25/44/2045		015 2045 5744
Poolise anni org	application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30559423. References: Qualcomm QC-CR#1060554.	25/11/2016	9.3	CVE-2016-6741
google android	An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privile	25/11/2016	9.3	CVE-2016-6742
google android	a privilege or process, variona IU. R-30.79982.8. An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising	25/11/2016	9.3	CVE-2016-6743
google android	a privileged process. Android ID: A-30937462. An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious	25/11/2016	0.2	
Poorbic sum onn	application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android 10: A-30970485. An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious	23/11/2010	9.3	CVE-2016-6744
google android	application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-31252388.	25/11/2016	9.3	CVE-2016-6745
google android	A denial of service vulnerability in Mediaserver in Android before 2016-11-05 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-31244612. References: NVIDIA N-CVE-2016-6747.	25/11/2016	7.1	CVE-2016-6747
	THE PARTY OF LOAD WAY.		•	

Semana 21/11/2016

Semana 21/11/2016						
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info		
google android	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflushing the operating system to repair the device. Android ID: A-39504789. References: NVIDION N-CVE-2016-6732.	25/11/2016	9.3	CVE-2016-6730		
google android	An elevation of privilege valuesability in the MVDIA OPU driver in Android before 2016-11-05 could enable a local multicious application to execute arbitrary code within the colored of the kernel. This sixe is rated as Cificial due to the possibility of a local permented durks compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906023, References: NVDION NCVL-2016-67313.	25/11/2016	9.3	CVE-2016-6731		
google android	An elevation of privilege vulnerability in the NVDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the content of the kernel. This sues is rated as Critical due to the possibility of a local permanent device compromise, which may require refliashing the operating system to repair the device. Android ID: A-30906599. References: NVIOIA NCVI-C306-6732.	25/11/2016	9.3	CVE-2016-6732		
google android	An elevation of privilege vulnerability in the NVDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the content of the kernel. This sues is rated as Critical due to the possibility of a local permanent device compromise, which may require refliashing the operating system to repair the device. Android ID: A-30906694. References: NVIOIA NCVIC-2016-6733.	25/11/2016	9.3	CVE-2016-6733		
google android	An elevation of privilege vulnerability in the NVDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the content of the kernel. This sues is rated as Critical due to the possibility of a local permanent device compromise, which may require refliashing the operating system to repair the device. Android ID: A-30907120. References: NVDIA NVC-IP-0316-6734.	25/11/2016	9.3	CVE-2016-6734		
google android	An elevation of privilege vulnerability in the NVDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the content of the kernel. This sues is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-39937701. Beferences: NVDIA NCV-C-2016-673S.	25/11/2016	9.3	CVE-2016-6735		
google android	An elevation of privilege vulnerability in the NVDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the content of the kernel. This suse is raised as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID. A-30553284. References: NVDIA NVCV-2-056-6738.	25/11/2016	9.3	CVE-2016-6736		
ge bently_nevada_3500/22m_serial_firmware	General Electric (GE) Bently Nevada 3500/22M USB with firmware before 5.0 and Bently Nevada 3500/22M Serial have open ports, which makes it easier for remote attackers to obtain privileged access via unspecified vectors.	24/11/2016	10.0	CVE-2016-5788		
lbmrational_team_concert	BM Rational Collaborative Lifecycle Management 3.0.1.6 before Fix8, 4.0 before 4.0.7 Fix11, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix6, Rational Quality Manager 3.0.1.6 before Fix4, 4.0 before 4.0.7 Fix11, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0 Fix6, Rational Feator Content 3.0.1.6 before Fix 6.0 before 4.0.7 Fix11, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix6, Rational Feator Content 3.0.1 before 5.0.2 Fix18, before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix18, Rational Rational Feator 6.0 Fix15, 5.0 before 5.0.2 Fix18, Fix18, and 6.0 before 6.0.2 Fix18, and 6.0 before 6.	24/11/2016	<u>7.5</u>	CVE-2016-0325		
ibm security_access_manager	IBM Security Access Manager for Web 7.0 before IF2 and 8.0 before 8.0.1.4 IF3 and Security Access Manager 9.0 before 9.0.1.0 IF5 allow remote authenticated users to execute arbitrary commands by leveraging LMI admin access.	24/11/2016	9.0	CVE-2016-3028		
libtiff – libtiff	tif_pixarlog.c in libiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "Pixarlog horizontal Difference heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9533		
libtiff libtiff	If write, in libit 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aks "TIFFFlushData1 heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9534		
libtiff libtiff	It predict hand figredict in light 3.0 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka "Predictor heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9535		
libtiff – libtiff	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka "t2p_process_jpeg_strip heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9536		
libtiff libtiff	as masw 33000, and Tap process typeg surprises pourier over now. tooks/fiffcrop.c in libitiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097. 35097.	22/11/2016	<u>7.5</u>	CVE-2016-9537		
libtiff – libtiff	tools/tiffcrop.c in libtiff 4.0.6 reads an undefined buffer in readContigStripsIntoBuffer() because of a uint16 integer overflow. Reported as MSVR 35100.	22/11/2016	<u>7.5</u>	CVE-2016-9538		
libtiff libtiff	tools/tiffcrop.c in libtiff 4.0.6 has an out-of-bounds read in readContigTilesIntoBuffer(). Reported as MSVR 35092.	22/11/2016	7.5	CVE-2016-9539		
libtiff – libtiff	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka "cpStripToTile heap-buffer-overflow."	22/11/2016	7.5	CVE-2016-9540		
paloaltonetworks pan-os	Buffer overflow in the management web interface in Palo Alto Networks PAN-OS before 5.0.20, 5.1.x before 5.1.13, 6.0 x before 6.0.15, 6.1.x before 6.1.15, 7.0 x before 7.0.11, and 7.1.x before 7.1.6 allows remote attackers to execute arbitrary code via unspecified vectors.	19/11/2016	10.0	CVE-2016-9150		

Semana 14/11/2016

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
linux linux_kernel	Theext4_journal_stop function in fs/ext4/ext4_jbd2.c in the Linux kernel before 4.3.3 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging improper access to a certain error field.	16/11/2016	9.3	CVE-2015-8961
inux linux_kernel	Double free vulnerability in the sg_common_write function in drivers/scsi/sg.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (memory corruption and system crash) by detaching a device during an SG_IO ioctl call.	16/11/2016	9.3	CVE-2015-8962
linux linux_kernel	Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an owevent data structure during a CPU unplug operation.	16/11/2016	<u>7.6</u>	CVE-2015-8963
linux linux_kernel	The tty_set_termios_Idisc function in drivers/tty/tty_Idisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure.	16/11/2016	<u>7.1</u>	CVE-2015-8964
inux linux_kernel	Use-after-free vulnerability in the disk_seqf_stop function in block/genhd.c in the Linux kernel before 4.7.1 allows local users to gain privileges by leveraging the execution of a certain stop operation even if the corresponding start operation had failed.	16/11/2016	9.3	CVE-2016-7910
linux linux_kernel	Race condition in the get_task_ioprio function in block/ioprio.c in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted ioprio_get system call.	16/11/2016	9.3	CVE-2016-7911
linux linux_kernel	Use-after-free vulnerability in the ffs_user_copy_worker function in drivers/usb/gadget/function/f_fs.c in the Linux kernel before 4.5.3 allows local users to gain privileges by accessing an I/O data structure after a certain callback call.	16/11/2016	9.3	CVE-2016-7912
inux linux_kernel	The xc2028_set_config function in drivers/media/funers/funer-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure.	16/11/2016	9.3	CVE-2016-7913
inux linux_kernel	The assoc_array_insert_into_terminal_node function in Big/assoc_array_c in the Linux kernel before 4.5.3 does not check whether a stot is a ledi, which allow social users to obtain sensitive information from kernel memory or cause a definal of service (breading ionited dereference and out-of-bounds read) via an application that uses associative-array data structures, as demonstrated by the keyutilis test suite.	16/11/2016	7.1	CVE-2016-7914
inux linux_kernel	Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/*/environ file during a process-setup time interval in which environment-variable copying is incomplete.	16/11/2016	7.1	CVE-2016-7916
emc avamar_data_store	EMC Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) versions 7.3 and older contain a vulnerability that may expose the Avamar servers to potentially be compromised by malicious users.	15/11/2016	7.2	CVE-2016-0909
exponentcms exponent_cms	In framework/modules/notfound/controllers/notfoundController.php of Exponent CMS 2.4.0 patch1, untrusted input is passed into get SearchResults. The method getSearchResults is defined in the search model with the parameter 'Sterm' used directly in SQL Impact is a SQL injection.	15/11/2016	<u>7.5</u>	CVE-2016-9287
objective_development little_snitch	Little Snitch version 3.0 through 3.6.1 suffer from a buffer overflow vulnerability that could be locally exploited which could lead to an escalation of privileges (EoP) and unauthorised ringb access to the operating system. The buffer overflow is related to insufficient checking of parameters to the "OSMAIloc" and "Copyin" kernel API calls.	15/11/2016	2.2	CVE-2016-8661
dotcms dotcms	SQL injection vulnerability in the categoriesServlet servlet in dotCMS before 3.3.1 allows remote not authenticated attackers to execute arbitrary SQL commands via the sort parameter.	14/11/2016	<u>7.5</u>	CVE-2016-8902
exponentcms exponent_cms	In framework/modules/navigation/controllers/navigation/Controller.php in Exponent CMS v2.4.0 or older, the parameter "target" of function "DragnDropReRaint" is directly used without any filtration which caused SQL injection. The payload can be used like this: //navigation/DragnDropReRaint/harpet/1.	11/11/2016	<u>7.5</u>	CVE-2016-9288
samsung samsung_mobile	Integer overflow in SystemUI in KK(4.4) and L(5.0/5.1) on Samsung Note devices allows attackers to cause a denial of service (UI restart) via vectors involving APIs and an activity that computes an out-of-bounds array index, aka SVE-2016-6906.	11/11/2016	<u>7.8</u>	CVE-2016-9277

	Semana 07/11/2016				
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info	
microsoft windows_10	The Common Log File System (LLFs) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows S1, Windows S1, Windows S1, Windows SP2, W	10/11/2016	9.3	CVE-2016-0026	
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows SL, Windows SP2 2012 Gold and R2, Windows R7 8.1, Windows 10 Gold, 1511, and 1607), and Windows Server 2016 allows Local users being privileges via a critical application, six Privileges Vision Service (Service System Service Service) of Privilege Vision Enable Vision Common Service (Service Service) (Service Service) (Service Service) (Service Service) (Service) (Service	10/11/2016	9.3	CVE-2016-3332	
microsoft windows_10	The Common Log File System (LLTS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows S F1, Windows Server 2016 and R2 SP1, Windows SP2 and R2 SP2, windows SP2 and R2	10/11/2016	9.3	CVE-2016-3333	
microsoft windows_10	The Common Log File System (LLTS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows S F1, Windows St. Windows SP2 and R2 SP1, windows SP2 and R2 SP2, windows SP2 and R2 SP2 and R	10/11/2016	9.3	CVE-2016-3334	
microsoft windows_10	The Common Log File System (LLTS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows S F1, Windows Server 2016 and R2 SP1, Windows SP2 and R2 SP2, windows SP2 and R2	10/11/2016	9.3	CVE-2016-3335	
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows S 75P1, Windows SL, Windows Server 2016 and R2, Windows SP2 and R2 SP1, Windows SP2 and R2 SP1, Windows SP2 and R2 SP1, Windows SP2 and R2 SP2, Mindows SP2 and R2 SP2 and R	10/11/2016	<u>9.3</u>	CVE-2016-3338	
microsoft windows_10	The Common Log File System (LLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows S 75P1, Windows S1, W	10/11/2016	9.3	CVE-2016-3340	

Driman Vander Dradust	Resolution	Dublished	CV/55 54050	Course & Batch Info
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
microsoft windows_10	The Common Log File System (LCIS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 15 Clost 1, SP2, Windows 15 Clost 1, SP2, and R2 SP2, Windows SP2 Clost 1, and 1620, and Windows Server 2016 SP2 and R2 SP2, Windows SP2 Clost 1, and 1620, and Windows Server 2016 allows Iscal users to gain privileges via a crafted application, alsa "Windows Common Log File System Driver Elevation of Privilege Visiterability," a different valuerability than CVE 2016-605C, CVE 2016-3332, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3334, CVE-2016-3334, CVE-2016-3335, CVE-2016-3355, CVE-2016-	10/11/2016	9.3	CVE-2016-3342
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows SP2,	10/11/2016	9.3	CVE-2016-3343
microsoft windows_10	The Common Log File System (CLFs) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows St. Windows Server 2016 and R2, Windows SP2 SP2, Windows R7 E1, Windows SP2 SP2, Windows SP2, Windows SP2, Windows SP2, Windows SP2, Windows SP2, Windows SP2, and Windows SP2, with Windows SP2, and Windows SP2, with Windows SP2, with Windows SP2, with Windows SP2, and Windows SP2, with Wind	10/11/2016	9.3	CVE-2016-7184
microsoft – edge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, alsa "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability on CV-2016-1938.	10/11/2016	<u>7.6</u>	CVE-2016-7195
microsoft edge	Nicrosoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a craffed web site, aka "Microsoft Browser Memory Corruption Vulnerability."	10/11/2016	7.6	CVE-2016-7196
microsoft edge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different	10/11/2016	7.6	CVE-2016-7198
	vulnerability than CVE-2016-7195. The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service			
microsoft edge	Inemony corruption) via a crafted web site, as a "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7244, and CVE-2016-7243. The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service	10/11/2016	7.6	CVE-2016-7200
microsoft edge	(memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.	10/11/2016	7.6	CVE-2016-7201
microsoft edge	The Chaira JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability", a different vulnerability than CVE- 2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243.	10/11/2016	<u>7.6</u>	CVE-2016-7202
microsoft edge	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a cartied web site. als "cripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7202, CVE-2016-7204, CVE-2016-7204, CVE-2016-7204, CVE-2016-7204.	10/11/2016	<u>7.6</u>	CVE-2016-7203
microsoft – edge	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-	10/11/2016	<u>7.6</u>	CVE-2016-7208
microsoft excel	2016-7200, CVF-2016-7201, CVF-2016-7202, CVF-2016-7203, CVF-2016-7240, CVF-2016-7242, and CVF-2016-7242. Microsoft Exet Got O7-89, Exet 2010 252, Exet 2013 SP1, Exet 2013 RT SP1, Exet 2016, Exet for Max 2011, Exet 2016 for Max, and Office Compatibility Pack SP3 allow rendoe attackers to execute arbitrary code via a rarlhed Office document, als 7 Microsoft Office	10/11/2016	9.3	CVE-2016-7213
microsoft windows_10	Memory Corruption Vulnerability." The kernel-mode drivers 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 R1 R3, Windows S10 Gold, 1511, and 1607, and Windows Server 2016 sillow local users to	10/11/2016	7.2	CVF-2016-7215
	gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." Input Method Editor (IME) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1,			
microsoft windows_10	Windows Server 2012 Gold and R.Z., Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles DLI loading, which allows local users to gain privileges via unspecified vectors, alsa "Windows ME Elevation of Privilege Vulnerability." Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a	10/11/2016	7.2	CVE-2016-7221
microsoft windows_10	Task Scheduler in Microsoft Windows 10 Gold, 15.11, and 1607 and Windows Server 2010 allows local users to gain privileges via a crafted UNC pathname in a task, aka "Task Scheduler Elevation of Privilege Vulnerability." Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, and	10/11/2016	7.2	CVE-2016-7222
microsoft excel	Microsoft Excel 2007-574, Excel 2010 572, Excel 2013 571, Excel 2013 N 1571, Excel 2010, Excel 2010 Mac. 2011, Excel 2010 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7228
microsoft excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka	10/11/2016	9.3	CVE-2016-7229
microsoft office_web_apps	"Microsoft Office Memory Corruption Vulnerability." Microsoft PowerPoint 2010 SP2, PowerPoint Viewer, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code	10/11/2016	9.3	CVE-2016-7230
microsoft excel	via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Microsoft Excel 2007 SP3, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7231
microsoft – office	arbitrary code via a crafted Uffice document, air "Microsoft Uffice Memory Corruption Vulnerability." Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, air "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7232
microsoft — excel_for_mac	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word 2013 SP9, Word 2013 RT SP1, Word for Mac 2011, Excel for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary of wait cardioted Office Comment, as a "Microsoft Office Memory Comption Vulnerability."	10/11/2016	9.3	CVE-2016-7234
microsoft excel_for_mac	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption	10/11/2016	9.3	CVE-2016-7235
microsoft – excel	Vulnerability." Microsoft Excel 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7236
microsoft - windows_10	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, Windows 10 Gold, 1511, and 1007, and Windows Server 2016 mishandle caching for NTUA password-change respects, which above local last on Early privileges via a rather application, as A "Vindows NTUAL Testivino of Privilege Vindows Institute Vindows NTUAL Testivino of Privilege Vindows NTUAL Testivino of	10/11/2016	7.2	CVE-2016-7238
microsoft edge	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a cartfed web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-201	10/11/2016	<u>7.6</u>	CVF-2016-7240
microsoft edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	10/11/2016	7.6	CVE-2016-7241
microsoft – edge	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service intensory corruption lyvia a crafted web site, ata "Scripting Engine Memory Corruption Volinerability" and ifferent vulnerability than CVE-2006-P200, CVE-2016-P200, CVE-2	10/11/2016	7.6	CVE-2016-7242
microsoft – edge	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, alse "scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CVE-061-7201, CVE-2016-7202, CVE-2016-7302, CVE-2016-7302, CVE-3016-7302, CVE-301	10/11/2016	7.6	CVF-2016-7243
microsoft – office	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, also "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7245
microsoft windows_10	The kernel-mode drivers in Microsoft Windows Server 2008 R 2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1807, and Windows Server 2016 allow local users to gain privileges via a crafted againstation, as "Online 2 Elevation of Privilege Vulnerability."	10/11/2016	7.2	CVE-2016-7246
microsoft windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow bocal users to gain privileges via a carted application, and *Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow bocal users to gain privileges via a carted application, and *WindoWindows Of Pivilege Vulnerability,"	10/11/2016	7.2	CVE-2016-7255
adobe flash_player	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.	08/11/2016	10.0	CVE-2016-7857
adobe flash_player	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.	08/11/2016	10.0	CVE-2016-7858
adobe flash_player	Adobe Flash Player versions 23.00.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.	08/11/2016	10.0	CVE-2016-7859
adobe flash_player	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.0.0.25 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability.	08/11/2016	10.0	CVE-2016-7860
adobe flash_player	Adobe Flash Player versions 23.00.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.00.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful	08/11/2016	10.0	CVE-2016-7861
adobe flash_player adobe flash_player	exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful	08/11/2016 08/11/2016	10.0	CVE-2016-7862 CVE-2016-7863
adobe flash player	exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful	08/11/2016	10.0	CVE-2016-7864
adobe flash_player	exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Surgestful exploitation could lead to arbitrary code awarution.	08/11/2016	10.0	CVE-2016-7865
nvidia geforce_experience	Successful exploitation could leaf to arbitrary code execution. For the NVIDIA Capidary, NVS, and Geforce products, GFG GameStream and NVTray Plugin unquoted service path vulnerabilities are examples of the unquoted service path vulnerability in Windows. A successful exploit of a vulnerable service installation can enable malicious code to execute on the system at the system/user privilege level. The CV-2016-316.10 is of the GameStream unquoted	08/11/2016	7.2	CVE-2016-3161
nvidia gpu_driver	service path. For the NVIDIA Quadro, NVS, and GeForce products, there is a Remote Desktop denial of service. A successful exploit of a vulnerable	08/11/2016	7.8	CVE-2016-4959
nvidia geforce_experience	system will result in a kernel null gointer dereference, causing a blue screen crash. For the NVIDA Capidor, NVS, and Geforce products, GFG BameFram and NVTray Plugin unquoted service path vulnerabilities are examples of the unquoted service path vulnerability in Windows. A successful exploit of a vulnerable service installation can enable malicious code to execute on the system at the system/user privilege level. The CVC 2016 SSS 210 b for the NVTray Plugin unquoted service.	08/11/2016	7.2	CVE-2016-5852
nvidia gpu_driver	service path. For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a valentability in the kernel mode layer (middmkm.ys) handler for DogDdfiszape where a user input to index an array is not	08/11/2016	7.2	CVE-2016-7381
nvidia gpu_driver	Dounds checked, leading to denial of service or potential escalation of privileges. For the WVDIA Quadro, NVS, GeForce, and Tesla products, NVDIA GPU Display Driver contains a vulnerability in the kernel mode layer myddfmm, sys for Windows or wids also for Linuxly handles where a missing permissions check may allow users to gain access to	08/11/2016	7.2	CVE-2016-7382
nvidia gpu_driver	arbitrary ohysical memory. leading to an escalation of crivilenes. For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kerner mode layer (indidation, xy) where unchecked input/output lengths in UVMLiteController Device	08/11/2016	7.2	CVE-2016-7384
nvidia gpu_driver	IO Control handling may lead to denial of service or potential exclashion of privileges. For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Diplay Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (invidentime, says) handler for DigDdfEscape ID 0x700010d where a value passed from a	08/11/2016	7.2	CVE-2016-7385
nvidia gpu_driver	user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of arribidese. For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 322.00 and 8375 before 375.63 contains a vulnerability in the kernel mode layer (invidentim, say) handler for DisplayIdificacye till occordionates without the text of the control of the product of the product of the control o	08/11/2016	7.2	CVE-2016-7387
	user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of crivileees.	,, -040		

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
nvidia gpu_driver	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (mvlddmkm.xys) handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential excalation of privileges.	08/11/2016	7.2	CVE-2016-7388
nvidia gpu_driver	For the NYIOLA Quadro, NYS, Geforce, and Tesla products, NYIOAA GPU localey Oriver on Linux R304 before 304.132, R340 before 340.38, R367 before 345.75, R361, 936 before 364.036, R367 before 364.000 contains a vulnerability in the kernel model layer (Invidia. ko) handler for mmap) where improper input validation may allow users to gain access to arbitrary physical memory, leading to an escalation of privileges.	08/11/2016	7.2	CVE-2016-7389
nvidia gpu_driver	For the NYIDM, Quadro, NYS, and GeForce products, NYIDM, Windows, GPU Display Driver (\$430 before \$42.00 and 8375 before \$75.63 contains a vulnerability in the kerne mode layer fividefining, ray) handler for Displatificacy to Di	08/11/2016	7.2	CVE-2016-7390
nvidia gpu_driver	For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (invidentim.sys) handler for Displotiscaper ID 0x100010b where a missing array bounds checks call above assert or write to kernel memory. Localing to derial of zervice or potential section of privilege.	08/11/2016	7.2	CVE-2016-7391
nvidia gpu_driver	For the NYIOLA Quadro, NYS, and GeForce products, NYIOLA Windows GPU Display Driver (\$430 before \$42.00 and 8375 before \$75.63 contains a vulnerability in the kerne mode layer (middimus, rays) handler for Displatificacy to (Displatificacy to (Displatificacy to (Displatificacy) to (Displatificacy) and (Singlatificacy) and (08/11/2016	7.2	CVE-2016-8805
nvidia gpu_driver	For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (invidentim.xys) handler for DxgDdiSzaper 10 DxGD0022V where a pointer passed from an user to the driver is used without voldidation, leading to desiral of service or proteinal seculation of privileges.	08/11/2016	7.2	CVE-2016-8806
nvidia gpu_driver	For the NVIDM Quadro, NVS, and GeForce products, NVIDM Windows GPU Display Oriver R340 before \$42.00 and R375 before \$75.63 contains a vulnerability in the kernel mode layer fivind/man, ray) handler for DisplatEscape ID Disciology-where a value is passed from an user to the driver is used without validation as the size input to memcpy() causing a stack buffer overflow, leading to denial of service or potential escalation of privileges.	08/11/2016	7.2	CVE-2016-8807
nvidia gpu_driver	For the NYIOLA Quadro, NYS, and GeForce products, NYIOLA Windows GPU Display Driver (\$430 before \$43.00 and 8375 before \$75.63 contains a vulnerability in the kerne mode layer (middimus, rays) handler for (poliptica;age IO). OXPOSIOS where a value passed from an user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges.	08/11/2016	7.2	CVE-2016-8808
nvidia gpu_driver	For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Windows GPU Dipplay Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (invidentim.xys) handler for DisplotEscape 10 D/10001b2 where the size of an input buffer in on visidate, loading to define of Service or potential escalation of privilege.	08/11/2016	7.2	CVE-2016-8809
nvidia gpu_driver	For the NYIOLA Quadro, NYS, and GeForce products, NYIOLA Windows GPU Display Driver (R300 before 842.00 and R375 before 375.63 contains a vulnerability in the kerne mode layer fividefinancy spl anotifier for productive specific productions and surpressed from an user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges.	08/11/2016	7.2	CVE-2016-8810
nvidia gpu_driver	For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Windows GPU Dipplay Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (invidentim.xys) handler for Displotis.cape 10 D/1000170 where the size of an input buffer in on visidate, loading to define of Service or potential escalation of privilege.	08/11/2016	7.2	CVE-2016-8811
nvidia geforce_experience	For the NVIDIA Quadro, NVS, and Geforce products, NVIDIA Geforce Experience R340 before GFE 2.11.4.125 and R375 before GFE 3.1.0.52 contains a vulnerability in the kernel mode layer (invitreamkins, sys) allowing a user to cause a stack buffer overflow with specially carfact executable parts, leading to a denial of service or exclastion of privileges.	08/11/2016	7.2	CVE-2016-8812
joomla joomla!	The register method in the UsersModelRegistration class in controllers/user.php in the Users component in Joomlal before 3.6.4 allows remote attackers to gain privileges by leveraging incorrect use of unfiltered data when registering on a site.	04/11/2016	<u>7.5</u>	CVE-2016-8869