Semana 28/11/2016

Primary Vendor Product	Semana 28/11/2016 Pescription	Published	CVSS Score	Source & Patch Info
bmc patrol	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 a binary named "virsh" using the PATh environment variable. The "listguests64" program will then run "virsh" using root privileges.	02/12/2016	7.2	CVE-2016-9638
ibm tivoli_monitoring	This allows local users to elevate their orivileaces to root. 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 eain orivileaces 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	30/11/2016	8.5	CVE-2016-2876
anager dell – idrac7_firmware	makes it easier for remote authenticated users to obtain root access by leveraging a command-injection issue. Dell iDRAC7 and iDRAC8 devices with firmware before 2.40.40.40 allow authenticated users to gain Bash shell access through a string	29/11/2016	9.0	CVE-2016-5685
exponentcms exponent_cms	injection. 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-loanam's Content in 'Usued direction' Iso. Oli, inacist is a Sol, inection.	29/11/2016	7.5	CVE-2016-9481
nginx nginx	The rigins packages or 16.2-5-4-6-6-6-7 as 3.6. impacts a 3.6. inscream. The rigins packages before 1.4.5-5-10-but 14.04 LTS, before 1.10.0-0-but 10.0-10-10-0-but 15.0-0-11.5 and before 1.10.0-0-but 10.15 in 15.0 allow local users with access to the web server user account to gain root principless via a synthia tasks on the error packages.	29/11/2016	7.2	CVE-2016-1247
canonical ubuntu_linux	The overlayfs implementation in the linux (aka Linux kernell) 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 configuration in which overlayfs is permitted in an arthur yrmount namespace.	27/11/2016	7.2	CVE-2015-1328
linux linux_kernel	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 minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heapbased buffer overflow) by leveraging the CAP NET ADMIN capability.	27/11/2016	7.2	CVE-2016-8632
linux linux_kernel	drivers/fino/pci/yfino_pci.ci in the Linux kernel through 4.8.1.1 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_INQS local:	27/11/2016	7.2	CVE-2016-9083
linux linux_kernel	security/keys/flig_key_c in the Linux kernel before 4.8.7 mishandles unsuccesful 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 unspecified other impact via a crafted application that uses the big_key data type.	27/11/2016	9.3	CVE-2016-9313
linux linux_kernel	The stop_sf_orb function in rel/sttp/sm_statefums.ci in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, 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	The _get_user_asm_ex macro in arch/s66/incluse/asm/usaccess, in the Linux kernel 4.4.22 through 4.4.22 Excitatise extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a crafted application. NOTE: this vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels.	27/11/2016	9.3	CVE-2016-9644
google android	An elevation of privilege vulnerability in Biopiples in Android 4.x before 4.4.5.0.x before 5.0.2, and 5.1.x before 5.10. could enable a local millicious application to execute affairs crode within the context of a privilege process. This issue to retail a Critical deal be to the possibility of a local permanent device compromise, which may require reflushing the operating system to repair the device. Android (b. A.29016186).	25/11/2016	9.3	CVE-2016-6700
google android	An elevation of privilege vulnerability in Medisserver in Android A. a before 4.4.4, 5.0.x before 5.1.5, 6.x before 5.1.6, i. b. before 5.1.6.1.1.0., and 7.0 before 20.5.1.5 i. b. clore 20.5.1.2 before 5.1.6.1.0.0 before 5.0.7	25/11/2016	9.3	CVE-2016-6704
google android	An elevation of privilege volumerability in Medisserveri in Antiroid 5.01 x before 5.02_5.1.x before 5.11_6.x before 2016-11.01, and 7.0 before 2016-11.02 could enable a local medicious application to execute arbitrary once within the control or a privileged process in Similar to Could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android 5033005721.	25/11/2016	9.3	CVE-2016-6705
google android	An elevation of privilege vulnerability in System Server in Android & x before 2016-11-01 and 7.0 before 2016-1-10 could enable a local mallicious application to execute arbitrary code within the context of a privileged process. This loss is rated at slife 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- 13390622.	25/11/2016	9.3	CVE-2016-6707
google android	A remote denial of service vulnerability in Mediaserver in Android S. s 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 denial of service. Android ICD. A-3082275S.	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 peccality 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-31992462.	25/11/2016	7.1	CVE-2016-6714
google android	An elevation of privilege vulnerability in Mediaserver in Android As before 4.4.4, 5.0x before 5.1.6, 5.5 before 5.1.6, before 5.1.6. before 5.1. before 5.1.6. before 5.1	25/11/2016	7.6	CVE-2016-6717
google android	A demial of service vulnerability in the Input Manager Service in Android 4.4. A 5.0 x before 5.0.2, 5.1 x before 5.1.1, 6.x before 5.0.2, 5.1 x b	25/11/2016	7.1	CVE-2016-6724
google android	Aremote code execution vulnerability in the Quaktomm crypto driver in Android before 2016-11-05 could enable a remote attacker to sexucite arbitrary code within the context of the kernel. This loss is raided scificial use to the possibility of remote code execution in the context of the kernel. Android ID. A-30515053. References: Quaktomm QC-CR81050970.	25/11/2016	10.0	CVE-2016-6725
google android	An elevation of privilege vulnerability in the kernel foll Nulbuystem in Androids before 2016-11-05 could enable a local miskicous application to execute arbitrary code which the context of the sent. This issue is related as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android Dr. A-30400942. An elevation of privilege vulnerability in the Qualstorma bootsdare's in Android before 2016-11-05 could enable a local miscious.	25/11/2016	9.3	CVE-2016-6728
google android	application to execute arbitrary code within the context of the terred. This cour is rated as Critical due to the possibility of a local permanent device components, which may require reflaching the operating system to repair the device. Android ID. A. 10977990. References: Qualcomm QC, C89977864. An elevation of privilege vulnerability in the NYDIA CPU driver in Android before 2016-11-05 could enable a local malicious application.	25/11/2016	9.3	CVE-2016-6729
google android	to execute stability code within the context of the served. This issue is rated as Critical data to the possibility of a local permanent excise compromise, which may require effashing the operating system to repair the device. Android ID. A 3004789. References: NYIOBA N.CVE-2016-6730. An elevation of privilege vulnerability is the NYIOBA CPU driver in Android before 2016-1-105 could enable a local mislicious application.	25/11/2016	9.3	CVE-2016-6730
google android	to execute whitney code within the context of the seriest. This issue is rated as Critical date to the possibility of a local permanent device compromise, which may require effashing the operating system to repair the device. Android ID. A. 30060232. References: NYIOLA N. CVI. 2016. 6731. An elevation of privilege vunderability in the NYIOLA CPU driver in Android before 2016-1-105 could enable a local mislicious application.	25/11/2016	9.3	CVE-2016-6731
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-30906599. References: NVIDIA N-CVE-2016-6732.	25/11/2016	9.3	CVE-2016-6732
google android	An elevation of privilege vulnerability in the NVDIA OFU driver in Android before 2016-11-05 could enable a local mislicious application to execute arbitrary code within the context of the kernel. This issue is rated as Cificial due to the possibility of a local permented device compromise, which may require reflashing the operating system to repair the device. Android ID. A. 30006694. References: NVDIO Nr. CVL-2-0566-6733.	25/11/2016	9.3	CVE-2016-6733
google android	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local multicious spilication to execute arbitrary code within the content of the kernel. This issue is rated as Cittical to be the possibility of bootal permanent device compromise, which may require relitating the operating system to repair the device. Android DRIVER STANDIAN EVENT STA	25/11/2016	9.3	CVE-2016-6734
google android	to execute arbitrary code within the context of the kernet. 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-30907701. References: NVIDIA N-CVE-2016-6735.	25/11/2016	9.3	CVE-2016-6735
google android	An elevation of privilege vulnerability in the NVIDIA OFU driver in Android before 2016-11-05 could enable a local mislicious application to execute arbitrary code within the context of the kernel. This sixes in stard as Circlia due to the possibility of a local permented device compromise, which may require reflashing the operating system to repair the device. Android ID. A 30953284. References: NVIOIA NCVL-2016-6736.	25/11/2016	9.3	CVE-2016-6736
google android	An elevation of privilege vulnerability in the kernel ION subsystem in Androids before 2016-11-05 Could enable a local misticous application to securite arbitrary code which the context of the kernel. This issue 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 IO: 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 contest of the benefi. This issue is rated as high because it first requires compromising a privileged process. Android ID: A-30034511. References: Qualcomm QC-CR#1050538.	25/11/2016	9.3	CVE-2016-6738
google android	An elevation of privilege value-shills; in the Quaktomic america driver in Android before 2016-11-05 could enable a local malicious application to securite arbitrary code white in the context of the server. This issue is readed a High because it first requires compromising a privileged process. Android ID: A-30074605. References: Quaktomin QC-CR81048926.	25/11/2016	9.3	CVE-2016-6739
google android	An elevation of privilege vulnerability in the Quasicomm camera driver in Android before 2016-11-05 could enable a local multicious application to execute arbitrary code within the contect 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 winerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious application to severule arbitrary code within the contect of the betwent. This know 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 touchtureen 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 privileged process. Android ID: A-30799828.	25/11/2016	9.3	CVE-2016-6742
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 privileged process. Android 10: A-30937462.	25/11/2016	9.3	CVE-2016-6743
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 privileged process. Android ID: A:39070485.	25/11/2016	9.3	CVE-2016-6744
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 if first requires compromising a privileged process. Android ID. A 31252388. A detail of Service vulnerability in Mediserver in Android before 2016-11-05 could enable an attacker to use a specialty crafted file to	25/11/2016	9.3	CVE-2016-6745
google android	in Lemian In Service values balany Tri Necusides en in invitol du Deriore 2009-1750. Codiu crisiale al indudecti us de 6 a specially classification in cause a device hange 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

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 INVIDIA GPU 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 Critical due to the possibility of a local permanent device compromise, which may require reliashing the operating system to repair the device. Android ID: A-39001789. References: NVIDIA NCVE-2016-6730.	25/11/2016	9.3	CVE-2016-6730
google android	An elevation of privilege vulnerability in the NVDIA OFU driver in Android before 2016-11-05 could enable a local multicious aggination to execute arbitrary code within the contract of the kernel. This issue is rated as Circlaid use to the possibility of a local permented device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906023. References: NVIOIA N-CVC-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 2016-11-25 could enable a local malicious application to execute arbitrary code within the context of the kernel. This sizes 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: NVIDIA NCVE-2016-6732.	25/11/2016	9.3	CVE-2016-6732
google android	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-25 could enable a local malicious application to execute arbitrary code within the context of the kernel. This sizes 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-39056694. References: NVIDIA NCVE-2016-6733.	25/11/2016	9.3	CVE-2016-6733
google android	An elevation of privilege vulnerability in the NVDIA OFU driver in Android before 2016-11-05 could enable a local multicious application to execute arbitrary code within the context of the kernel. This issue is rated as Circla due to the possibility of a local permented device compromise, which may require reflashing the operating system to repair the device. Android ID: A-39007120. References: NVDION A-VCV-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 2016-11-25 could enable a local malicious application to execute abilityra code within the context of the kernel. This sues is rated as Critical due to the possibility of a local permanent device compromise, which may require refliathing the operating system to repair the device. Android ID: A-30907701. References: NVIDIA NCVE-2016-6735.	25/11/2016	9.3	CVE-2016-6735
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 content of the kernel's linis use 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-30553284. References: NVIDIA NCVE-2016-6738.	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
ibmrational_team_concert	BIM National 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 Fix5, Rational Couliny 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 6.0.2 Fix5, Rational Fixed Concerns 3.0.1 before 1.0.4 before 4.0.7 Fix11, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix6, Rational Fixed Concerns 4.0.0 before 4.0.7 Fix11, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix6, Rational Rational Fixed Concerns 4.0.2 Fix15, 5.0 before 5.0.2 Fix18, and 6.0 before 6.0.2 Fix18, and 6.0 befo	24/11/2016	7.5	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 libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "PixarLog horizontalDifference heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9533
libtiff – libtiff	tif_write.c in libtiff 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, aka "TiFFFlushData1 heap-buffer-overflow."	22/11/2016	<u>7.5</u>	CVE-2016-9534
libtiff libtiff	If_predict.h and tif_predict.c in libtiff 4.0.6 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 libitiff 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	7.5	CVE-2016-9536
libtiff – libtiff	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097.	22/11/2016	7.5	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	The _ext4_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
linux 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 loctl 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 swevent 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_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
linux 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/loprio.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
linux linux_kernel	The xx2028_set_config function in drivers/medis/tuners/tuner-xx2028.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
linux linux_kernel	The saso_array_insert_into_lerminal_node function in Bilyasoc_array_c in the Linux kernel before 4.5.3 does not heck whether a stot is a kell, which allows local 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 keyutils test suite.	16/11/2016	<u>7.1</u>	CVE-2016-7914
linux 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/notfound/controller.php of Exponent CMS 2.4.0 patch1, untrusted input is passed into getSearchResults. 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 "OSMIAIC" and "Copyin" kernel APIC Little Copyin Little 2014 (1994).	15/11/2016	7.2	CVF-2016-8661
dotems dotems	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	7.5	CVE-2016-8902
exponentcms exponent_cms	In framework/modules/navigation/controllers/navigationController.php in Exponent CNS v2.4.0 or older, the parameter "target" of function 'DragnDropReRamir' is directly used without any filtration which caused SQL injection. The payload can be used like this: //navigation/DragnDropReRamir.pared11.	11/11/2016	<u>7.5</u>	CVE-2016-9288
samsung samsung_mobile	Integer overflow in SystemUI in KK(4.4) and U(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	7.8	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 (CLFs) driver in Microsoft Windows Volta 5P2, Windows Server 2008 5P2 and R2 5P1, Windows 7 5P1, Windows 8.1, Windows 15 were 2016 691 and R2, Windows 16 8.1, Windows 16 0.004, 1511, and 1607, and Windows 5 erver 2016 691 allows local users to gain privileges via a critical application, ask "Mindows Common Log File System Driver Evention of Privilege Vulnerability," a different vulnerability than CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-335, CVE-2016	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 SL1, Windows SP2 06 Gold, 1511, and 1607), and Windows Server 2016 allows local users to gain privileges via a critical epilation, in all Windows Common Log File System Driver Elevation of Privilege Valuerability, a different vulnerability than CVE-2016-0026, CVE-2016-3313, CVE-	10/11/2016	9.3	CVE-2016-3332
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SPZ, Windows Server 2008 SPZ and R2 SPI, Windows S 7 SPI, Windows SL, Windows SPC 2012 Gold and R2, Windows R7 SL, Windows SPC B0 Gold, 1511, and 1807), and Windows Server 2016 slowless Color and the gain privileges was a related application, sits "Artivolose Common Log File System Evire Elevation of Privilege Valuerability," a different vulnerability than CVE 2016-0026, CVE 2016-3332, CVE-2016-3333,	10/11/2016	9.3	CVE-2016-3333
microsoft windows_10	The Common Log File System (CLTS) driver in Microsoft Windows Vista SPZ, Windows Server 2008 SPZ and R2 SPI, Windows S 7 SPI, Windows SL, Windows SPC 2012 Gold and R2, Windows R1 SL, Windows SPC BO, GOLD, TSPI, and SPG 3, and Windows Server 2016 slowless Cell on the Disp microllegs via a critical application, six 3 revivaes Cell Cell Service Servic	10/11/2016	9.3	CVE-2016-3334
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SPZ, Windows Server 2008 SPZ and R2 SPI, Windows S 7 SPI, Windows SL, Windows SPC 2012 Gold and R2, Windows R7 SL, Windows SPC B0 Gold, 1511, and 1807), and Windows Server 2016 slowless Color and the gain privileges was a related application, sits "Artivolose Common Log File System Evire Elevation of Privilege Valuerability," a different vulnerability than CVE 2016-0026, CVE 2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3344, CVE-2016-3344, CVE-2016-3344, CVE-2016-3344,	10/11/2016	9.3	CVE-2016-3335
microsoft windows_10	The Common Log File System (CLFS) driver in Microsoft Windows Vista SPZ, Windows Server 2008 SPZ and R2 SPI, Windows S 7 SPI, Windows SL, Windows SPC 2012 Gold and R2, Windows R1 SL, Windows X1 GOLD, 15 Li, and 1807), and Windows Server 2016 allows local uses to gain privileges via a raided appliation, lask "Mindows Common Leg The System Driver Evision of Privilege Vulnerability," a different vulnerability than CVE 2016 GOZ, CVE 2016-3332, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3355, CVE-2016-3355, CVE-2016-3355, CVE-2016-3355, CVE-2016-335	10/11/2016	9.3	CVE-2016-3338
microsoft windows_10	The Common Log File Syntem (CLTs) driver in Microsoft Windows Vida SPZ, Windows Server 2008 SPZ and RZ SPI, Windows S FI, Windows SL, Windows SPZ 2012 Gold and RZ, Windows RT 8.1, Windows 10 Gold, 1511, and 1607), and Windows Server 2016 allows local users to gain privileges via a raided appliation, i.a.8 Vindows Common Log File System Evher Elevation of Privilege Vulnerability, a different vulnerability than CVX -2016 GOZ, CVX -2016-3332, CVX -2016-3333, CVX -2016-3333, CVX -2016-3333, CVX -2016-3334, CVX -2016-3344, CX -2016-3344, CX -2016-3344, CX -2016-3344, CX -2016-3344, CX -20	10/11/2016	9.3	CVE-2016-3340

Discontinuity Design	B. California	Bulliote d	01000	Common State Late
Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
microsoft windows_10	The Common Log File System (LSI) driver in Microsoft Windows Vida SP2, Windows Server 2008 SP2 and R2 SP1, Windows SP3 SP3, Windows SP3, Windows SP2, Windows SP3, Windows SP2, Windows SP2	10/11/2016	9.3	CVE-2016-3342
microsoft windows_10	The Common Log File System (CLFs) driver in Microsoft Windows Votas 572, Windows Server 2008 592 and R2 591, Windows 7 591, Windows 51, Windows 51, Windows 52, Wi	10/11/2016	9.3	CVE-2016-3343
microsoft windows_10	The Common Ling Elicystem (LIS) drive in Microsoft Windows Vida 5/21, Windows Server 2008 5/2 and R2 5/11, Windows 7 5/11, Windows S. Windows Server 2016 5/2 and R2 5/11, Windows 1, Windo	10/11/2016	9.3	CVF-2016-7184
microsoft – edge	AUTO-3348, CVE-2016-3340, CVE-2016-3342, am UVE-2016-3343. Microsoft Interret Explored 9 through 1 and Microsoft Interret page allow remote attackers to execute arbitrary code or cause a denial of service imemory corruption is a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability with CV 2016-7198.	10/11/2016	7.6	CVE-2016-7195
microsoft edge	suinterability than CVE-1010-1198. Microsoft 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 crafted 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
microsoft – edge	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 (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-	10/11/2016	7.6	CVE-2016-7200
microsoft – edge	2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a demial of service (memory corruption via a crafted web site, akia "Scripting Engine Memory Corruption Viaherability," a different vulnerability than CVE-2016-7200, CVE-2016	10/11/2016	7.6	CVE-2016-7201
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	7.6	CVE-2016-7202
microsoft edge	2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. The Chairx JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service memory corruspion via a craftler whe site, as a "Scripting regine Memory Corruspion Vulnerability," a different vulnerability than CVE-	10/11/2016	7.6	CVE-2016-7203
-	2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, 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			
microsoft edge	Imemory corruption) via a crafted 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-2016-7204, CVE-2016-7242, and CVE-2016-7243. Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 SP1, Excel 2013 SP2, Excel 2013 SP3, Ex	10/11/2016	7.6	CVE-2016-7208
microsoft excel	Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." 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,	10/11/2016	9.3	CVE-2016-7213
microsoft windows_10	Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	10/11/2016	7.2	CVE-2016-7215
microsoft windows_10	Input Method Editor (IME) in Microsoft Windows Visia SP2, Windows Server 2008 SP2 and 82 SP1, Windows SP1, Windows 8.1, Windows SP2, Windows SP3, Windows SP3, Windows SP3, Windows SP3, Windows SP3, Windows 16 G04, MS14 in a 1609, and Windows Server 2016 methodate DL loading, which allows local users to gain privileges via unspecified vectors, also "Windows IME Elevation of Privilege Vulnerability."	10/11/2016	7.2	CVE-2016-7221
microsoft windows_10	Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a crafted UNC pathname in a task, aka "Task Scheduler Elevation of Privilege Vulnerability."	10/11/2016	<u>7.2</u>	CVE-2016-7222
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, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office	10/11/2016	9.3	CVE-2016-7228
microsoft excel	Memory Corruption 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, 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 Memory Corruption Vulnerability." Microsoft PowerPoint 2010 SP2, PowerPoint Viewer, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code			
microsoft office_web_apps	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	10/11/2016	9.3	CVE-2016-7230
microsoft excel	arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers	10/11/2016	9.3	CVE-2016-7231
microsoft office	Microsoft Word 2007, Office 2010 \$92, Word 2010 \$92, Word 2013 \$91, Word 2013 RT \$91, Word for Mac 2011, Excel for Mac 2011,	10/11/2016	9.3	CVE-2016-7232
microsoft excel_for_mac	Mort 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2010 SP3 and Office Web Apps Server 2013 SP3 allow remote attackers to execute arbitrary code via a crafted Office document, also "Microsoft Office Memory Corruption Vulnerability". Microsoft Word 2010, Office 2010 SP2, Word 2010 SP2, Word of to Mac 2011, Excel for Mac 2011, and Office Compatibility Pack SP3	10/11/2016	9.3	CVE-2016-7234
microsoft excel_for_mac	NICrosoft Word 2007, Unite 2010 SP2, Word 2010 SP2, Word for Niez 2011, Excellor Misc 2011, and Unite 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-2016-7235
microsoft excel	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 8.1.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows SP SP2, SP3, Windows SP2, Windows SP3, Windows S	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 carted web site, alsa "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7302, CVE-201	10/11/2016	7.6	CVE-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 (memory corruption) via a carled web site, als "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CV-2016-7201, CV-2016-720, CV-2016-7302, CV-2016-7302, CV-2016-7302, GV-2016-7302, GV-2016-7302, CV-2016-7302, GV-2016-7302, CV-2016-7302, GV-2016-7302, CV-2016-7302, GV-2016-7302,	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 carted web site, als "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE- 2016-7200, CV-2016-7201, CV-2016-7202, CV-2016-7208,	10/11/2016	7.6	CVE-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, aka "Microsoft Office Memory Corruption Vulnerability."	10/11/2016	9.3	CVE-2016-7245
microsoft windows_10	The kernel-made drivers in Microsoft Windows Server 2008 R.2.5°L, Windows 7.5°P., Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows Gold 1.5°L, and 1.0°C, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win328 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 SP2 and R2 SP1, Windows SP2 and R2 SP1, Windows R2 A1, Windows II Gibl, ISS1, and ISS7, and Windows Server 2016 allow local users to gain privileges via carried application, and Wind2 IXE endon of Privilege Vulnerability."	10/11/2016	<u>7.2</u>	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. Adoba Clash Player versions 2.0.025 and earlier, 11.2.026.643 and earlier have an exploitable type confusion vulnerability.	08/11/2016	10.0	CVE-2016-7860
adobe flash_player	Adobe Flash Player versions 23.0.0.205 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 23.0.0.205 and earlier, 11.202.643 and earlier have an exploitable use-after-free vulnerability. Successful	08/11/2016	10.0	CVE-2016-7861
adobe flash_player	exploitation could lead to arbitrary code execution.	08/11/2016	10.0	CVE-2016-7862
adobe flash_player	Adobe Flish 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. Adobe Flish 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-2016-7863
adobe flash_player	Adobe Hish Player versions 23.00.005 and earner, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. Adobe Flash Player versions 23.00.005 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability.	08/11/2016	10.0	CVE-2016-7864
adobe flash_player	Adobe Hish Player versions 25.00.205 and earlier, 11.2.202.b43 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. For the NVIDIA Quadro, NVS, and GeForce products, GFE GameStream and NVTray Plugin unquoted service path vulnerabilities are	08/11/2016	10.0	CVE-2016-7865
nvidia geforce_experience	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 CVE-2016-3161 ID is for the GameStream unquoted service path.	08/11/2016	<u>7.2</u>	CVE-2016-3161
nvidia gpu_driver	service parn. For the NYIDIA Quadro, NYS, and Geforce products, there is a Remote Desktop denial of service. A successful exploit of a vulnerable system will result in a kernel null pointer dereference, causing a blue screen crash.	08/11/2016	7.8	CVE-2016-4959
nvidia geforce_experience	Steelth Bild Bild and set of the second seco	08/11/2016	7.2	CVE-2016-5852
nvidia gpu_driver	Service (MIDI). For the NVIDIA Quadrio, 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 (nviddmkm.xys) handler for DigDdEscape where a user input to index an array is not bounds checked, locating to derival of service or potential sections of privilege.	08/11/2016	7.2	CVE-2016-7381
nvidia gpu_driver	For the NVIDIA Cardin, NWS, Gef-Fore, and Tesla products, NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer (middmkn, sys for Windows or midia ao for Linus) handler where a missing permissions check may allow users to gain access to arbitrare obviscial memory, leading to an escalation of conflictees.	08/11/2016	7.2	CVE-2016-7382
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 ternel mode layer (invidentine say) where unkneked input/output lengths in UVMLIBEController Device 100 Control handlering wise last doesied in Service or potential excelation of privilege.	08/11/2016	7.2	CVE-2016-7384
nvidia gpu_driver	For the NVIDIA CLUMEN, NOS, and Geffore products, NVIDIA Villedons GRD Display Detver RAD before 342.00 and KTST Selece 375.63 contains a vulnerability in the terred mode being refloridations, by harder for Display Except to Display Observe a value passed not user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of or invidence.	08/11/2016	7.2	CVE-2016-7385
	orwineses. For the NVDIJA 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 (nviddmkm.sys) handler for DxgDdiEscape ID 0x600000D where a value passed from a	08/11/2016	7.2	CVE-2016-7387
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			

Primary Vendor Product	Description	Published	CVSS Score	Source & Patch Info
vidia 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 (nviddmkm.sys) handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges.	08/11/2016	7.2	CVE-2016-7388
vidia gpu_driver	For the NYIDIA Quadro, NNS, GeForce, and Tesla products, NYIDIA GPU Display Driver on Linux R304 before 30.112, R340 before 340.98, R367 before 307.55, R361.39, before 361.59,012, and R370 before 370 cortains a vulnerability in the kernel mode layer (midd ia. O) 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
vidia gpu_driver	For the NVIDIA Quadro, NNS, and Geforce products, NVIDIA Windows GPU Display Driver R300 before \$42.00 and R375 before \$75.63 contains a vulnerability in the kernel mode layer (individuality) and large for globific sape (in Dixoro)394 where a value passed from a 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-2016-7390
vidia gpu_driver	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.53 contains a vulnerability in the sternel mode layer (invidentinas,ye)) ander for DagDdEscape 10 Dx1000100 where a missing array bounds check can allow a user to write to bernel memory, cleaning to definal of evicine or per	08/11/2016	7.2	CVE-2016-7391
vidia gpu_driver	For the NVIDIA Quadro, NNS, and Geforce products, NVIDIA Windows GPU Display Driver 8140 before 842.00 and 8375 before 375.63 contains a valeneability in the kernel mode layer (individuancy) handler for Oppditiscape to Discriptional 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-2016-8805
vidia 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 (middment.ye) handler for DugDdiEscape 10 0x500027 where a pointer passed from an user to the driver is used without validation, leading to define of benefit of section of privileges.	08/11/2016	7.2	CVE-2016-8806
vidia gpu_driver	For the NVIDIA Quadro, NXS, and Geforce products, NVIDIA Windows GPU Display Driver 8340 before 842.00 and 8375 before 375.63 contains a vulnerability in the kernel mode layer (individuancy) handler for polyatificacyae (in Oxcology) 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 operatil sculation of arthribes.	08/11/2016	7.2	CVE-2016-8807
vidia gpu_driver	For the NVIDIA Quadro, NNS, and Geforce products, NVIDIA Windows GPU Display Driver 8340 before 842.00 and 8375 before 375.63 contains a valeneability in the kernel mode layer (individuality) plantel for polydeficiscae (in DixnOxio05W 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
vidia 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 lexenter mode layer (windomfrance) in landler for Displit Expan (D 0.70001b2 where the size of an input buffer is not validated, leading to denial of service or potential exclusion of privileges.	08/11/2016	7.2	CVE-2016-8809
vidia gpu_driver	for the NVIDIA Quadro, NNS, and Geforce products, NVIDIA Windows GPU Display Driver R840 before 84.20 and R875 before 375.63 contains a vulnerability in the kernel mode layer (invidentiness) palmatifer for polydeficis, ape ID Oxfordios) 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-2016-8810
vidia 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 (invidamins.ys) handler for DisplitExcape 10 0x7000170 where the size of an input buffer is not validated, leading to denied of service or potential exclusion of privileges.	08/11/2016	7.2	CVE-2016-8811
vidia 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 (instremalms, sys) allowing a user to cause a stack buffer overflow with specially crafted exercible path, leading to a denial of service or exclasion of privileges.	08/11/2016	7.2	CVE-2016-8812
oomla 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