BGD e-GOV CIRT

BGD e-GOV CIRT project
Common Vulnerabilities and Exposures (CVE) Report

Issue Date: 02-January-2020 **Issue Number:02**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Microsoft				
Microsoft Windows Security Feature Bypass Vulnerability	12-NOV-2019	**9.9 Critical**	**CVE-2019-1384** A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages. To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1384
Microsoft Exchange Remote Code Execution Vulnerability	12-NOV-2019	**9.8 Critical**	**CVE-2019-1373** A remote code execution vulnerability exists in Microsoft Exchange through the deserialization of metadata via PowerShell, aka 'Microsoft Exchange Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1373
Microsoft Office ClickToRun Security Feature Bypass Vulnerability	12-NOV-2019	**9.8 Critical**	**CVE-2019-1449** A security feature bypass vulnerability exists in the way that Office Click-to-Run (C2R) components handle a specially crafted file, which could lead to a standard user, any AppContainer sandbox, and Office LPAC Protected View to escalate privileges to SYSTEM.To exploit this bug, an attacker would have to run a specially crafted file, aka 'Microsoft Office ClickToRun Security Feature Bypass Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1449
Win32k Graphics Remote Code Execution Vulnerability	10-DEC-2019	**8.8 High**	**CVE-2019-1468** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Win32k Graphics Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
OpenType Font Parsing Remote Code Execution Vulnerability	10-NOV-2019	**8.8 High**	**CVE-2019-1456** A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1456
Win32k Graphics Remote Code Execution Vulnerability	12-NOV-2019	**8.8 High**	**CVE-2019-1441** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Win32k Graphics Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1441
Windows Hyper-V Remote Code Execution Vulnerability	10-DEC-2019	**8.2 High**	**CVE-2019-1471** A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1471
NetLogon Security Feature Bypass Vulnerability	12-DEC-2019	**8.1 High**	**CVE-2019-1424** A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1424
Windows OLE Remote Code Execution Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1484** A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1484
Windows Elevation of Privilege Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1476** An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1476

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Windows Elevation of Privilege Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1483** An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1483
Windows COM Server Elevation of Privilege Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1478** An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1478
Microsoft PowerPoint Remote Code Execution Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1462** A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly handle objects in memory, aka 'Microsoft PowerPoint Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1462
Win32k Elevation of Privilege Vulnerability	10-DEC-2019	**7.8 High**	**CVE-2019-1458** An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1458
Microsoft Excel Remote Code Execution Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1448** A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1448
Microsoft Windows Media Foundation Remote Code Execution Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1430** A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'Microsoft Windows Media Foundation Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1430

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Windows Elevation of Privilege Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1423** An elevation of privilege vulnerability exists in the way that the StartTileData.dll handles file creation in protected locations, aka 'Windows Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1423
Scripting Engine Memory Corruption Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1429** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429
Windows Installer Elevation of Privilege Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1415** An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1415
Windows Graphics Component Elevation of Privilege Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1407** An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1407
Windows UPnP Service Elevation of Privilege Vulnerability	12-NOV-2019	**7.8 High**	**CVE-2019-1405** An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1405
Remote Desktop Protocol Information Disclosure Vulnerability	10-DEC-2019	**7.5 High**	**CVE-2019-1489** An information disclosure vulnerability exists when the Windows Remote Desktop Protocol (RDP) fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to connect remotely to an	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1489

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			affected system and run a specially crafted application.	
VBScript Remote Code Execution Vulnerability	10-DEC-2019	**7.5 High**	**CVE-2019-1485** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1485
Application: McAfee				
McAfee Client Proxy update fixes Web Gateway bypass vulnerability	13-NOV-2019	**8.6 High**	**CVE-2019-3654** Authentication Bypass vulnerability in the Microsoft Windows client in McAfee Client Proxy (MCP) prior to 3.0.0 allows local user to bypass scanning of web traffic and gain access to blocked sites for a short period of time via generating an authorization key on the client which should only be generated by the network administrator.	https://kc.mcafee.com/corporate/index?page=content&id=SB10305
McAfee Total Protection, McAfee Anti-Virus Plus, and McAfee Internet Security version 16.0.R22 Refresh 1 fixes a privilege escalation vulnerability	13-NOV-2019	**6.7 Medium**	**CVE-2019-3654** McAfee Total Protection, McAfee Anti-Virus Plus, and McAfee Internet Security version 16.0.R22 Refresh 1 fixes a privilege escalation vulnerability A Privilege Escalation vulnerability in the Microsoft Windows client in McAfee Total Protection 16.0.R22 and earlier allows administrators to execute arbitrary code via carefully placing malicious files in specific locations protected by administrator permission.	https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS102984

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Cisco				
Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution Vulnerability	06-NOV-2019	**9.8 CRITICAL**	**CVE-2019-15958** A vulnerability in the REST API of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an unauthenticated remote attacker to execute arbitrary code with root privileges on the underlying operating system. The vulnerability exists because affected devices with the High Availability (HA) feature enabled do not properly perform input validation. An attacker could exploit this vulnerability by uploading a malicious file to either the HA active or standby device. A successful exploit could allow the attacker to execute arbitrary code with root-level privileges on the underlying operating system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-pi-epn-codex
Cisco Web Security Appliance Unauthorized Device Reset Vulnerability	06-NOV-2019	**8.8 High**	**CVE-2019-15956** A vulnerability in the web management interface of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform an unauthorized system reset on an affected device. The vulnerability is due to improper authorization controls for a specific URL in the web management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could have a twofold impact: the attacker could either change the administrator password, gaining privileged access, or reset the network configuration details, causing a denial of service (DoS) condition. In both scenarios, manual intervention is required to restore normal operations.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wsa-unauth-devreset
Cisco TelePresence Collaboration Endpoint, TelePresence Codec, and RoomOS	06-NOV-2019	**8.8 High**	**CVE-2019-15288** A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE), Cisco TelePresence Codec (TC), and Cisco RoomOS Software could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Software Privilege Escalation Vulnerability			allow an authenticated, remote attacker to escalate privileges to an unrestricted user of the restricted shell.The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including specific arguments when opening an SSH connection to an affected device. A successful exploit could allow the attacker to gain unrestricted user access to the restricted shell of an affected device.	20191106-telepres-roomos-privesc
Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Arbitrary Command Execution Vulnerability	06-NOV-2019	**8.8 High**	**CVE-2019-15271** A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The attacker must have either a valid credential or an active session token. The vulnerability is due to lack of input validation of the HTTP payload. An attacker could exploit this vulnerability by sending a malicious HTTP request to the web-based management interface of the targeted device. A successful exploit could allow the attacker to execute commands with root privileges.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbrv-cmd-x
Cisco Unified Communications Manager SQL Injection Vulnerability	20-NOV-2019	**8.8 High**	**CVE-2019-15972** A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates SQL values. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to modify	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-cucm-sql

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			values on or return values from the underlying database.	
Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities	06-NOV-2019	**7.8 HIGH**	**CVE-2019-15283 CVE-2019-15284 CVE-2019-15285 CVE-2019-15286 CVE-2019-15287** Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system.The vulnerabilities exist due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-webex-player
Cisco DNA Spaces: Connector Command Injection Vulnerability	20-NOV-2019	**6.7 MEDIUM**	**CVE-2019-15997** vulnerability in Cisco DNA Spaces: Connector could allow an authenticated, local attacker to perform a command injection attack and execute arbitrary commands on the underlying operating system as root.The vulnerability is due to insufficient validation of arguments passed to a specific CLI command. An attacker could exploit this vulnerability by including malicious input during the execution of the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as root.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-dna-cmd-injection

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Huawei				
Buffer Overflow Vulnerability in Some Huawei Smart Phones	23-DEC-2019	**8.8 HIGH**	Huawei smart phones with earlier versions than ELLE-AL00B 9.1.0.222(C00E220R2P1) have a buffer overflow vulnerability. An attacker may intercept and tamper with the packet in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause the affected phone abnormal.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-02-smartphone-en
Huawei products (AP2000;IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; S5700; SVN5600; SVN5800; SVN5800-C; SeMG9811; Secospace AntiDDoS8000; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG6000V; eSpace U1981)	13-DEC-2019	**8.6 HIGH**	**CVE-2019-5254** **CVE-2019-5255** **CVE-2019-5256** **CVE-2019-5257** **CVE-2019-5258** Certain Huawei products (AP2000;IPS Module; NGFW Module; NIP6300; NIP6600; NIP6800; S5700; SVN5600; SVN5800; SVN5800-C; SeMG9811; Secospace AntiDDoS8000; Secospace USG6300; Secospace USG6500; Secospace USG6600; USG6000V; eSpace U1981) have an out-of-bounds read vulnerability. An attacker who logs in to the board may send crafted messages from the internal network port or tamper with inter-process message packets to exploit this vulnerability. Due to insufficient validation of the message, successful exploit may cause the affected board to be abnormal.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191211-01-ssp-en
Vulnerabilities in Some Huawei Home Routers	29-NOV-2019	**8.1 HIGH**	**CVE-2019-5268** **CVE-2019-5269** Some Huawei home routers have an input validation vulnerability. Due to input parameter is not correctly verified, an attacker can exploit this vulnerability by sending special constructed packets to obtain files in the device and upload files to some directories.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191113-01-homerouter-en

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Weak Algorithm Vulnerability in Some Huawei Products	13-DEC-2019	**7.5 HIGH**	**CVE-2019-19397** There is a weak algorithm vulnerability in some Huawei products. The affected products use weak algorithms by default. Attackers may exploit the vulnerability to cause information leaks.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191204-01-vrp-en
Out-Of-Bound Read Vulnerability in Some Huawei Products	13-NOV-2019	**7.5 HIGH**	**CVE-2019-5294** There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191023-01-buffer-en
Insufficient Input Validation Vulnerability in Huawei Share	23-DEC-2019	**7.5 HIGH**	**CVE-2019-5266** Huawei Share function in P30 9.1.0.193(C00E190R2P1) smartphone has an insufficient input validation vulnerability. Attackers can exploit this vulnerability by sending crafted packets to the affected device. Successful exploit may cause the function will be disabled.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-02-share-en
Denial of Service Vulnerability in some Huawei Products	13-DEC-2019	**7.4 HIGH**	**CVE-2019-5248** CloudEngine 12800 has a DoS vulnerability. An attacker of a neighboring device sends a large number of specific packets. As a result, a memory leak occurs after the device uses the specific packet. As a result, the attacker can exploit this vulnerability to cause DoS attacks on the target device.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191204-03-dos-en
Information Disclosure Vulnerability in Some Huawei Products	23-DEC-2019	**5.5 MEDIUM**	**CVE-2019-5267** Huawei OceanStor SNS3096 V100R002C01 have an information disclosure vulnerability. Attackers with low privilege can exploit this vulnerability by performing some specific operations. Successful exploit of this vulnerability can cause some information disclosure.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-03-information-en

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Adobe				
Adobe Illustrator CC (APSB19-36) vulnerabilities	14-NOV-2019	**9.8 CRITICAL**	**CVE-2019-7962 CVE-2019-8247 CVE-2019-8248 CVE-2019-16447** Adobe Illustrator CC versions 23.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/illustrator/apsb19-36.html
Adobe Media Encoder (APSB19-52) Out-of-bounds Read Vulnerability	14-NOV-2019	**9.8 CRITICAL**	**CVE-2019-8241 CVE-2019-8242 CVE-2019-8243 CVE-2019-8244 CVE-2019-8246** Adobe Media Encoder versions 13.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/media-encoder/apsb19-52.html
Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability	25-OCT-2019	**9.8 CRITICAL**	**CVE-2019-8088** Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/experience-manager/apsb19-48.html
Adobe Photoshop CC (APSB19-56) Memory Corruption	19-DEC-2019	**7.8 HIGH**	**CVE-2019-8253 CVE-2019-8254** Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/photoshop/apsb19-56.html
Application: MOVEit				
MOVEit Transfer SQL Injection Vulnerability	31-OCT-2019	**9.8 CRITICAL**	**CVE-2019-18464** In Progress MOVEit Transfer 10.2 before 10.2.6 (2018.3), 11.0 before 11.0.4 (2019.0.4), and 11.1 before 11.1.3 (2019.1.3), multiple SQL Injection vulnerabilities have been found in the REST API that could allow an unauthenticated attacker to gain unauthorized access to the database. Depending on the database engine being used (MySQL, Microsoft SQL	https://community.ipswitch.com/s/article/SQL-Injection-Vulnerability-2

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database or may be able to alter the database.	
Application: Zend Framework				
Zend Framework: Potential SQL Injection Vector When Using PDO_MySql	26-NOV-2019	**9.8 CRITICAL**	**CVE-2011-1939** SQL injection vulnerability in Zend Framework 1.10.x before 1.10.9 and 1.11.x before 1.11.6 when using non-ASCII-compatible encodings in conjunction PDO_MySql in PHP before 5.3.6.	https://framework.zend.com/security/advisory/ZF2011-02
Application: PostgreSQL				
PostgreSQL: Unanticipated errors from the standard library.	26-NOV-2019	**9.8 CRITICAL**	**CVE-2015-3166** The snprintf implementation in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 does not properly handle system-call errors, which allows attackers to obtain sensitive information or have other unspecified impact via unknown vectors, as demonstrated by an out-of-memory error.	https://www.postgresql.org/about/news/1587/
Application: Samba				
Malicious servers can cause Samba client code to return filenames containing path separators to calling code.	06-NOV-2019	**6.5 MEDIUM**	**CVE-2019-10218** A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.	https://www.samba.org/samba/security/CVE-2019-10218.html

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Linux				
cyrus-imapd: privilege escalation in HTTP request	14-NOV-2019	**9.8 Critical**	**CVE-2019-18928** Cyrus IMAP 2.5.x before 2.5.14 and 3.x before 3.0.12 allows privilege escalation because an HTTP request may be interpreted in the authentication context of an unrelated previous request that arrived over the same connection.	https://www.cyrusimap.org/imap/download/release-notes/2.5/x/2.5.14.html https://www.cyrusimap.org/imap/download/release-notes/3.0/x/3.0.12.html
Linux Kernel up to 5.3.9 audit.c aa_label_parse() memory corruption	07-NOV-2019	**9.8 Critical**	**CVE-2019-18814** An issue was discovered in the Linux kernel through 5.3.9. There is a use-after-free when aa_label_parse() fails in aa_audit_rule_init() in security/apparmor/audit.c.	https://lore.kernel.org/patchwork/patch/1142523/
Heap overflow flaw	29-NOV-2019	**9.8 Critical**	**CVE-2019-14901** A heap overflow flaw was found in the Linux kernel, all versions 3.x.x and 4.x.x before 4.18.0, in Marvell WiFi chip driver. The vulnerability allows a remote attacker to cause a system crash, resulting in a denial of service, or execute arbitrary code. The highest threat with this vulnerability is with the availability of the system. If code execution occurs, the code will run with the permissions of root. This will affect both confidentiality and integrity of files on the system.	-
Linux kernel CIFS implementation	27-NOV-2019	**7.8 High**	**CVE-2019-10220** Linux kernel CIFS implementation, version 4.9.0 is vulnerable to a relative paths injection in directory entry lists.	Available in respective vendor web site.
Linux kernel 5.0.21	17-DEC-2019	**7.8 High**	**CVE-2019-19814** In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.	-

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Intel Linux Administrative Tools for Intel Network Adapters Vulnerability	16-DEC-2019	**7.8 High**	**CVE-2019-0159** Insufficient memory protection in the Linux Administrative Tools for Intel(R) Network Adapters before version 24.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00237.html
Linux kernel before 5.1.6	03-DEC-2019	**7.8 High**	**CVE-2019-19543** In the Linux kernel before 5.1.6, there is a use-after-free in serial_ir_init_module() in drivers/media/rc/serial_ir.c.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.1.6
Linux Kernel 5.0.21 btrfs Filesystem fs/btrfs/volumes.c __btrfs_map_block memory corruption	17-DEC-2019	**7.8 High**	**CVE-2019-19816** In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.	-
Linux kernel 4.19.83	12-DEC-2019	**7.5 High**	**CVE-2019-19770** In the Linux kernel 4.19.83, there is a use-after-free (read) in the debugfs_remove function in fs/debugfs/inode.c (which is used to remove a file or directory in debugfs that was previously created with a call to another debugfs function such as debugfs_create_file).	-
Linux kernel before 5.3.9	18-NOV-2019	**7.5 High**	**CVE-2019-19065** A memory leak in the sdma_init() function in drivers/infiniband/hw/hfi1/sdma.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering rhashtable_init() failures, aka CID-34b3be18a04e.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.9
Linux kernel before 5.3.4	18-NOV-2019	**7.5 High**	**CVE-2019-19081** A memory leak in the nfp_flower_spawn_vnic_reprs() function in drivers/net/ethernet/netronome/nfp/	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.4

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			flower/main.c in the Linux kernel before 5.3.4 allows attackers to cause a denial of service (memory consumption), aka CID-8ce39eb5a67a.	
Linux kernel before 5.3.9	03-DEC-2019	**6.8 Medium**	**CVE-2019-19532** In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.9
Linux kernel 5.0.21	17-DEC-2019	**5.5 Medium**	**CVE-2019-19815** In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsync_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h.	https://github.com/torvalds/linux/commit/4969c06a0d83c9c3dc50b8efcdc8eeedfce896f6#diff-41a7fa4590d2af87e82101f2b4dadb56
Application: Mikrotik				
MikroTik RouterOS < 6.44.6 LTS or 6.45.x < 6.45.7 Multiple Vulnerabilities	04-NOV-2019	**7.5 High**	**CVE-2019-3976** **CVE-2019-3977** The remote networking device is running a version of MikroTik RouterOS prior to 6.44.6 LTS or 6.45.x prior to 6.45.7 affected by multiple vulnerabilities : Relative Path Traversal in NPK Parsing - RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below are vulnerable to an arbitrary directory creation vulnerability via the upgrade package's name field. RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below insufficiently validate where upgrade	Upgrade to MikroTik RouterOS 6.44.6 LTS, 6.45.7 and later. https://forum.mikrotik.com/viewtopic.php?f=21&t=153379 https://forum.mikrotik.com/viewtopic.php?f=21&t=153378

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			packages are download from when using the autoupgrade feature. Insufficient Protections of a Critical Resource (DNS Requests/Cache) Improper DNS Response Handling	
Application:DLink				
D-Link DAP-1860 prior 1.04b03 Beta HTTP Header HNAP_AUTH Remote Code Execution<	04-DEC-2019	**8.8 High**	**CVE-2019-19597** D-Link DAP-1860 devices before v1.04b03 Beta allow arbitrary remote code execution as root without authentication via shell metacharacters within an HNAP_AUTH HTTP header.	-
Application: WordPress				
WordPress up to 5.3.0 HTML5 wp-includes/kses.php wp_kses_bad_protocol unknown vulnerability	27-DEC-2019	**9.8 Critical**	**CVE-2019-20041** wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript: substring.	Upgrading to version 5.3.1 https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53
Lever PDF Embedder Plugin 4.4 on WordPress PDF Document unknown vulnerability	04-DEC-2019	**8.8 Critical**	**CVE-2019-19589** The Lever PDF Embedder plugin 4.4 for WordPress does not block the distribution of polyglot PDF documents that are valid JAR archives.	https://wordpress.org/plugins/pdf-embedder/#developers
W3 Total Cache up to 0.9.2.4 on WordPress Hash Generation information disclosure	22-NOV-2019	**7.5 High**	**CVE-2012-6078** W3 Total Cache before 0.9.2.5 generates hash keys insecurely which allows remote attackers to predict the values of the hashes.	https://www.w3-edge.com/weblog/2013/01/security-w3-total-cache-0-9-2-4/
NextGEN Gallery up to 2.1.14 on WordPress directory traversal	26-NOV-2019	**6.5 MEDIUM**	**CVE-2015-9538** The NextGEN Gallery plugin before 2.1.15 for WordPress allows ../ Directory Traversal in path selection	https://wordpress.org/plugins/nextgen-gallery/#developers
Shortcode Ninja Plugin up to 1.4 on WordPress preview-shortcode-	27-DEC-2019	**6.1 MEDIUM**	**CVE-2014-4550** Cross-site scripting (XSS) vulnerability in preview-shortcode-external.php in the Shortcode Ninja plugin 1.4 and	-

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
external.php shortcode cross site scripting			earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the shortcode parameter.	
Application: CentOS				
CentOS Web Panel 0.9.8.856 through 0.9.8.864 vulnerability	17-DEC-2019	**6.5 Medium**	**CVE-2019-14782** CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.856 through 0.9.8.864 allows an attacker to get a victim's session file name from the /tmp directory, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to make a request to extract the victim's password (for the OS and phpMyAdmin) via an attacker account.	https://centos-webpanel.com/changelog-cwp7
CentOS Web Panel 0.9.8.864 vulnerability	17-DEC-2019	**6.5 Medium**	**CVE-2019-15235** CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.864 allows an attacker to get a victim's session file name from /home/[USERNAME]/tmp/session/sess_xxxxxx, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to gain access to the victim's password (for the OS and phpMyAdmin) via an attacker account.	https://centos-webpanel.com/changelog-cwp7
Application: Drupal				
Views Dynamic Fields Module up to 7.x-1.0-alpha4 on Drupal views_handler_filter_dynamic_fields.inc Remote Code Execution	16-DEC-2019	**9.8 CRITICAL**	**CVE-2019-19826** The Views Dynamic Fields module through 7.x-1.0-alpha4 for Drupal makes insecure unserialize calls in handlers/views_handler_filter_dynamic_fields.inc, as demonstrated by PHP object injection, involving a field_names object and an Archive_Tar object, for file deletion. Code execution might also be possible.	https://www.drupal.org/project/views_dynamic_fields/issues/3056600
Activity Module 6.x-1.x on Drupal cross site request forgery	21-NOV-2019	**8.8 High**	**CVE-2012-2079** A cross-site request forgery (CSRF) vulnerability in the Activity module 6.x-1.x for Drupal.	https://www.drupal.org/node/1506562

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Drupal 7.0/7.1/7.2/7.3/7.4 File Upload directory traversal	15-NOV-2019	**7.5 HIGH**	**CVE-2011-2726** An access bypass issue was found in Drupal 7.x before version 7.5. If a Drupal site has the ability to attach File upload fields to any entity type in the system or has the ability to point individual File upload fields to the private file directory in comments, and the parent node is denied access, non-privileged users can still download the file attached to the comment if they know or guess its direct URL.	Upgrading to version 7.5 https://www.drupal.org/node/1231510
Ckeditor Module 7.x-1.4 on Drupal hook_file_download Request information disclosure	13-NOV-2019	**7.5 HIGH**	**CVE-2011-4972** hook_file_download in the CKEditor module 7.x-1.4 for Drupal does not properly restrict access to private files, which allows remote attackers to read private files via a direct request.	https://drupal.org/node/1337006
SVG Sanitizer Module up to 8.x-1.0-alpha1 on Drupal denial of service	11-NOV-2019	**7.5 HIGH**	**CVE-2019-18856** A Denial Of Service vulnerability exists in the SVG Sanitizer module through 8.x-1.0-alpha1 for Drupal because access to external resources with an SVG use element is mishandled.	https://git.drupalcode.org/project/svg_sanitizer/commit/e1b0666
Views Builk Operations Module up to 6.x-1.0 on Drupal cross site scripting	25-NOV-2019	**6.1 MEDIUM**	**CVE-2011-3373** Drupal Views Builk Operations (VBO) module 6.x-1.0 through 6.x-1.10 does not properly escape the vocabulary help when the vocabulary has had user tagging enabled and the "Modify node taxonomy terms" action is used. A remote attacker could provide a specially-crafted URL that could lead to cross-site scripting (XSS) attack.	Upgrading the latest version.
Application: Apache				
Apache Tomcat: Low: Session fixation	23-DEC-2019	**9.8 CRITICAL**	CVE-2019-17563 When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side	- Upgrade to Apache Tomcat 9.0.30 or later - Upgrade to Apache Tomcat 8.5.50 or later - Upgrade to Apache Tomcat 7.0.99 or later

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			of caution, this issue has been treated as a security vulnerability.	https://lists.apache.org/thread.html/8b4c1db8300117b28a0f3f743c0b9e3f964687a690cdf9662a884bbd%40%3Cannounce.tomcat.apache.org%3E
Apache SpamAssassin up to 3.4.2 CF File privilege escalation	12-DEC-2019	**9.8 CRITICAL**	**CVE-2018-11805** In Apache SpamAssassin before 3.4.3, nefarious CF files can be configured to run system commands without any output or errors. With this, exploits can be injected in a number of scenarios. In addition to upgrading to SA 3.4.3, we recommend that users should only use update channels or 3rd party .cf files from trusted places.	Upgrading to version 3.4.3 https://svn.apache.org/repos/asf/spamassassin/branches/3.4/build/announcements/3.4.3.txt
Apache Olingo up to 4.6.0 Public API AbstractService privilege escalation	04-DEC-2019	**9.8 CRITICAL**	**CVE-2019-17556** Apache Olingo versions 4.0.0 to 4.6.0 provide the AbstractService class, which is public API, uses ObjectInputStream and doesn't check classes being deserialized. If an attacker can feed malicious metadata to the class, then it may result in running attacker's code in the worse case.	https://mail-archives.apache.org/mod_mbox/olingo-user/201912.mbox/%3CCAGSZ4d4vbSYaVh3aUWAvcVHK2qcFxxCZd3WAx3xbwZXskPX8nw%40mail.gmail.com%3E
Apache Solr 8.1.1/8.2.0 Configuration File solr.in.sh privilege escalation	18-NOV-2019	**9.8 CRITICAL**	**CVE-2019-12409** The 8.1.1 and 8.2.0 releases of Apache Solr contain an insecure setting for the ENABLE_REMOTE_JMX_OPTS configuration option in the default solr.in.sh configuration file shipping with Solr. If you use the default solr.in.sh file from the affected releases, then JMX monitoring will be enabled and exposed on RMI_PORT (default=18983), without any authentication. If this port is opened for inbound traffic in your firewall, then anyone with network access to your Solr nodes will be able to access JMX, which may in turn allow them to upload malicious code for execution on the Solr server.	https://lists.apache.org/thread.html/6640c7e370fce2b74e466a605a46244ccc40666ad9e3064a4e04a85d@%3Csolr-user.lucene.apache.org%3E

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Apache Xerces-C use-after-free vulnerability processing external DTD	18-DEC-2019	**7.5 High**	**CVE-2018-1311** The Apache Xerces-C 3.0.0 to 3.2.2 XML parser contains a use-after-free error triggered during the scanning of external DTDs. This flaw has not been addressed in the maintained version of the library and has no current mitigation other than to disable DTD processing. This can be accomplished via the DOM using a standard parser feature, or via SAX using the XERCES_DISABLE_DTD environment variable.	https://marc.info/?l=xerces-c-users&m=157653840106914&w=2
Apache Spam Assassin up to 3.4.2 Message Resource Exhaustion denial of service	12-DEC-2019	**7.5 High**	**CVE-2019-12420** In Apache Spam Assassin before 3.4.3, a message can be crafted in a way to use excessive resources. Upgrading to SA 3.4.3 as soon as possible is the recommended fix but details will not be shared publicly.	Upgrading to version 3.4.3 https://lists.apache.org/thread.html/e3c2367351286b77a74a082e2b66b793cceefa7b6ea9dcd162db4c4b@<dev.spamassassin.apache.org> https://svn.apache.org/repos/asf/spamassassin/branches/3.4/build/announcements/3.4.3.txt
Apache Shiro up to 1.4.1 Configuration Cookie Padding weak encryption	18-NOV-2019	**7.5 High**	**CVE-2019-12422** Apache Shiro before 1.4.2, when using the default "remember me" configuration, cookies could be susceptible to a padding attack.	https://lists.apache.org/thread.html/c9db14cfebfb8e74205884ed2bf2e2b30790ce24b7dde9191c82572c@%3Cdev.shiro.apache.org%3E
Application: Joomla				
Joomla CMS up to 3.9.13 Parameter sql injection	17-DEC-2019	**9.8 CRITICAL**	**CVE-2019-19846** In Joomla! before 3.9.14, the lack of validation of configuration parameters used in SQL queries caused various SQL injection vectors.	Upgrade to version 3.9.14. https://developer.joomla.org/security-centre/797-20191202-core-various-sql-injections-through-configuration-parameters

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
verot.net class.upload up to 2.0.4 File Extension class.upload.php privilege escalation	04-DEC-2019	**9.8 CRITICAL**	**CVE-2019-19634 CVE-2019-19576** class.upload.php in verot.net class.upload before 1.0.3 and 2.x before 2.0.4, as used in the K2 extension for Joomla! and other products, omits .phar from the set of dangerous file extensions.	https://www.verot.net/php_class_upload.htm
Shack Forms Pro Extension up to 4.0.31 on Joomla File Attachment directory traversal	09-OCT-2019	**9.8 CRITICAL**	**CVE-2019-17399** The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment.	https://www.joomlashack.com/changelog/shack-forms/
ProJoom Smart Flash Header up to 3.0.2 on Joomla views/upload.php Filename privilege escalation	18-NOV-2019	**8.8 HIGH**	**CVE-2014-1214** views/upload.php in the ProJoom Smart Flash Header (NovaSFH) component 3.0.2 and earlier for Joomla! allows remote attackers to upload and execute arbitrary files via a crafted (1) dest parameter and (2) arbitrary extension in the Filename parameter.	-
Application: VMware				
VMware Workstation/Fusion e1000e Virtual Network Adapter Out-of-Bounds memory corruption	20-NOV-2019	**9.1 CRITICAL**	**CVE-2019-5541** VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM.	https://www.vmware.com/security/advisories/VMSA-2019-0021.html
VMware Workstation/Fusion vmnetdhcp information disclosure	20-NOV-2019	**7.7 High**	**CVE-2019-5540** VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process.	https://www.vmware.com/security/advisories/VMSA-2019-0021.html

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
VMware Workstation/Fusion RPC denial of service	20-NOV-2019	**7.7 High**	**CVE-2019-5542** VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain a denial-of-service vulnerability in the RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM.	https://www.vmware.com/security/advisories/VMSA-2019-0021.html
Application: PHP				
phpfastcache up to 5.1.2 Cookie Driver privilege escalation	12-DEC-2019	**9.8 CRITICAL**	**CVE-2019-16774** In phpfastcache before 5.1.3, there is a possible object injection vulnerability in cookie driver.	Upgrading to version 5.1.3 https://github.com/PHPSocialNetwork/phpfastcache/commit/c4527205cb7a402b595790c74310791f5b04a1a4
suPHP up to 0.7.1 Source Highlighting Code Execution	13-DEC-2019	**7.8 High**	**CVE-2014-1867** suPHP before 0.7.2 source-highlighting feature allows security bypass which could lead to arbitrary code execution	Upgrading to version 0.7.2
phpMyChat-Plus 1.98 Password Reset URL pass_reset.php pmc_username cross site scripting	20-DEC-2019	**6.1 Medium**	**CVE-2019-19908** phpMyChat-Plus 1.98 is vulnerable to reflected XSS via JavaScript injection into the password reset URL. In the URL, the pmc_username parameter to pass_reset.php is vulnerable.	-
Application: Backdrop CMS				
phpMyChat-Plus 1.98 Password Reset URL pass_reset.php pmc_username cross site scripting	20-DEC-2019	**7.2 High**	**CVE-2019-19902** An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It allows the upload of entire-site configuration archives through the user interface or command line. It does not sufficiently check uploaded archives for invalid data, allowing non-configuration scripts to potentially be uploaded to the server. This issue is mitigated by the fact that the attacker would be required to have the "Synchronize, import, and export configuration" permission, a permission that only trusted administrators should be given.	Upgrading to version 1.13.5 or 1.14.2. https://backdropcms.org/security/backdrop-sa-core-2019-016

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			Other measures in the product prevent the execution of PHP scripts, so another server-side scripting language must be accessible on the server to execute code.	
Application: Contao				
Contao 4.0 through 4.8.5 unrestricted file uploads	17-DEC-2019	**8.8 High**	**CVE-2019-19745** Contao 4.0 through 4.8.5 allows PHP local file inclusion. A back end user with access to the form generator can upload arbitrary files and execute them on the server.	Update to Contao 4.4.46 or 4.8.6. https://contao.org/en/security-advisories/unrestricted-file-uploads.html
Application: Google				
Google Android	04-NOV-2019	**High**	Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for arbitrary code execution within the context of a privileged process. Details of these vulnerabilities are as follows: An arbitrary code vulnerability in Library. (CVE-2019-2201) An information disclosure vulnerability in Kernel components. (CVE-2019-11833) Multiple arbitrary code vulnerabilities in System. (CVE-2019-2204, CVE-2019-2205, CVE-2019-2206) Multiple elevation of privilege vulnerabilities in Framework. (CVE-2019-2192, CVE-2019-2193, CVE-2019-2195, CVE-2019-2199) Multiple elevation of privilege vulnerabilities in Kernel components. (CVE-2019-2213, CVE-2019-2214, CVE-2019-2215) Multiple elevation of privilege vulnerabilities in Media framework. (CVE-2019-2202, CVE-2019-2203) Multiple elevation of privilege vulnerabilities in System. (CVE-2019-2036, CVE-2019-2207, CVE-2019-2233) Multiple information disclosure vulnerabilities in Framework. (CVE-2019-2196, CVE-2019-2197, CVE-2019-2198, CVE-2019-2211)	http://source.android.com/security/bulletin/2019-11-01.html

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
			Multiple information disclosure vulnerabilities in System. (CVE-2019-2208, CVE-2019-2209, CVE-2019-2212) Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2019-10484, CVE-2019-10485, CVE-2019-10493, CVE-2019-10511, CVE-2019-10559, CVE-2019-2288, CVE-2019-2319, CVE-2019-2320, CVE-2019-2321, CVE-2019-2337, CVE-2019-2338) Multiple vulnerabilities in Qualcomm components. (CVE-2019-10545, CVE-2019-10571, CVE-2019-2310)	
Google Chrome prior 78.0.3904.87 WebAudio HTML Page Use-After-Free memory corruption	25-NOV-2019	**8.8 HIGH**	**CVE-2019-13720** Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	Upgrading to version 78.0.3904.87. https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

CV Scoring Scale (CVSS)	0	0.1-3.9	4-6.9	7-8.9	9-10
	None	Low	Medium	High	Critical