BGD e-GOV CIRT

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

Issue Date: 23-January-2020 **Issue Number:03**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Microsoft				
Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	14-JAN-2020	**9.8 CRITICAL**	**CVE-2020-0609** **CVE-2020-0610** A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610
.NET Framework Remote Code Execution Injection Vulnerability	14-JAN-2020	**9.8 CRITICAL**	**CVE-2020-0646** A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646
Windows CryptoAPI Spoofing Vulnerability	14-JAN-2020	**8.1 High**	**CVE-2020-0601** A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source, aka 'Windows CryptoAPI Spoofing Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
Microsoft Excel Remote Code Execution Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0653** **CVE-2020-0650** **CVE-2020-0651** A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0653

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
			objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0650 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0651
Microsoft Office Memory Corruption Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0652** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0652
Windows Elevation of Privilege Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0644** **CVE-2020-0635** An elevation of privilege vulnerability exists when Microsoft Windows implements predictable memory section names, aka 'Windows Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0644 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0635
Win32k Elevation of Privilege Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0642** **CVE-2020-0624** 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-2020-0642 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0624
Update Notification Manager Elevation of Privilege Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0638** An elevation of privilege vulnerability exists in the way the Update Notification Manager handles files.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Update Notification Manager Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0638

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 Common Log File System Driver Elevation of Privilege Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0634** An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0634
Windows Search Indexer Elevation of Privilege Vulnerability	14-JAN-2020	**7.8 HIGH**	**CVE-2020-0633, CVE-2020-0613, CVE-2020-0614, CVE-2020-0623, CVE-2020-0625, CVE-2020-0626, CVE-2020-0627, CVE-2020-0628, CVE-2020-0629, CVE-2020-0630, CVE-2020-0631, CVE-2020-0632** An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0633 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0613 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0614 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0623 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0625 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0626 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0627 https://portal.msrc.microsoft.com/en-US/security-

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
				guidance/advisory/CVE-2020-0628 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0629 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0630 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0631 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0632
Internet Explorer Memory Corruption Vulnerability	14-JAN-2020	**7.5 HIGH**	**CVE-2020-0640** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0640
Application: Citrix				
Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance	27-DEC-2019	**9.8 CRITICAL**	**CVE-2019-19781** An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	https://support.citrix.com/article/CTX267027
Authentication Bypass Vulnerability in the Management Interface of Citrix Application Delivery Controller and Citrix Gateway	21-OCT-2019	**9.8 CRITICAL**	**CVE-2019-18225** An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name.	https://support.citrix.com/article/CTX261055

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 Data Center Network Manager Authentication Bypass Vulnerabilities	02-JAN-2020	**9.8 CRITICAL**	**CVE-2019-15975 CVE-2019-15976 CVE-2019-15977** Multiple vulnerabilities in the authentication mechanisms of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-auth-bypass
Cisco Data Center Network Manager Command Injection Vulnerabilities	02-JAN-2020	**7.2 High**	**CVE-2019-15978 CVE-2019-15979** Multiple vulnerabilities in the REST and SOAP API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative privileges on the DCNM application to inject arbitrary commands on the underlying operating system (OS).	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-comm-inject
Cisco Data Center Network Manager SQL Injection Vulnerabilities	02-JAN-2020	**7.2 High**	**CVE-2019-15984 CVE-2019-15985** Multiple vulnerabilities in the REST and SOAP API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to execute arbitrary SQL commands on an affected device. To exploit these vulnerabilities, an attacker would need administrative privileges on the DCNM application.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-sql-inject
Cisco Data Center Network Manager Path Traversal Vulnerabilities	02-JAN-2020	**7.2 High**	**CVE-2019-15980 CVE-2019-15981 CVE-2019-15982** Multiple vulnerabilities in the REST and SOAP API endpoints and the Application Framework feature of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. To exploit these vulnerabilities, an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-path-trav

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
			attacker would need administrative privileges on the DCNM application.	
Application: Apache				
Apache cordova-plugin-inappbrowser CVE-2019-0219 Privilege Escalation Vulnerability	14-JAN-2020	**9.8 CRITICAL**	**CVE-2019-0219** A website running in the InAppBrowser webview on Android could execute arbitrary JavaScript in the main application's webview using a specially crafted gap-iab: URI.	https://lists.apache.org/thread.html/197482d5ab80c0bff4a5ec16e1b0466df38389d9a4b5331d777f14fc%40%3Cdev.cordova.apache.org%3E
Apache Solr RCE CVE-2019-0192	07-MAR-2019	**9.8 CRITICAL**	**CVE-2019-0192** In Apache Solr versions 5.0.0 to 5.5.5 and 6.0.0 to 6.6.5, the Config API allows to configure the JMX server via an HTTP POST request. By pointing it to a malicious RMI server, an attacker could take advantage of Solr's unsafe deserialization to trigger remote code execution on the Solr side.	http://mail-archives.us.apache.org/mod_mbox/www-announce/201903.mbox/%3CCAECwjAV1buZwg%2BMcV9EAQ19MeAWztPVJYD4zGK8kQdADFYij1w%40mail.gmail.com%3E https://lists.apache.org/thread.html/ec9c572fb803b26ba0318777977ee6d6a2fb3a2c50d9b4224e541d5d@%3Cdev.lucene.apache.org%3E
Apache Tomcat CVE-2019-17563 Session Fixation Vulnerability	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 of caution, this issue has been treated as a security vulnerability.	https://lists.opensuse.org/opensuse-security-announce/2020-01/msg00013.html https://lists.apache.org/thread.html/8b4c1db8300117b28a0f3f743c0b9e3f964687a690cdf9662a884bbd%40<announce.tomcat.apache.org>
Apache Log4j CVE-2019-17571 Deserialization Remote Code	20-DEC-2019	**9.8 CRITICAL**	**CVE-2019-17571** Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which	https://lists.apache.org/thread.html/44491fb9cc19acc901f7cff34acb7376619f15

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
Execution Vulnerability			can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.	638439416e3e14761c@<dev.tika.apache.org> https://lists.apache.org/thread.html/479471e6debd608c837b9815b76eab24676657d4444fcfd5ef96d6e6@<dev.tika.apache.org> https://logging.apache.org/log4j/2.x/
Apache Xerces-C CVE-2018-1311 Remote Code Execution Vulnerability	18-DEC-2019	**8.1 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://lists.apache.org/thread.html/r48ea463fde218b1e4cc1a1d05770a0cea34de0600b4355315a49226b@<c-dev.xerces.apache.org>
Apache Solr CVE-2019-17558 Remote Code Execution Vulnerability	30-DEC-2019	**7.5 High**	**CVE-2019-17558** Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).	http://www.apache.org https://lucene.apache.org/solr/

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 SpamAssassin up to 3.4.2 CF File privilege escalation	12-DEC-2019	**6.7 Medium**	**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://lists.apache.org/thread.html/6f89f82a573ea616dce53ec67e52d963618a9f9ac71da5c1efdbd166@<users.spamassassin.apache.org> https://lists.apache.org/thread.html/0b5c73809d0690527341d940029f743807b70550050fd23ee869c5e5@<users.spamassassin.apache.org>
Application: Samba				
Samba Releases Security Updates	21-JAN-2020	**6.5 Medium**	**CVE-2019-19344** There is a use-after-free issue in all samba 4.9.x versions before 4.9.18, all samba 4.10.x versions before 4.10.12 and all samba 4.11.x versions before 4.11.5, essentially due to a call to realloc() while other local variables still point at the original buffer.	https://www.samba.org/samba/security/CVE-2019-19344.html
Samba Releases Security Updates	21-JAN-2020	**6.5 Medium**	**CVE-2019-14907** All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process (such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).	https://www.samba.org/samba/security/CVE-2019-14907.html
Samba Releases Security Updates	21-JAN-2020	**5.4 Medium**	**CVE-2019-14902** There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba	https://www.samba.org/samba/security/CVE-2019-14902.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
			4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.	
Application: Oracle				
Oracle WebLogic Server Vulnerability	15-JAN-2020	**9.8 CRITICAL**	**CVE-2020-2551** Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpujan2020.html
Oracle Solaris 10 Common Desktop Environment unknown vulnerability	15-JAN-2020	**8.8 High**	**CVE-2020-2696** Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris.	https://www.oracle.com/security-alerts/cpujan2020.html
Oracle Security Updates	15-JAN-2020	**7.5 High**	**CVE-2020-2726** Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.36, prior to 6.0.16 and prior to 6.1.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the	https://www.oracle.com/security-alerts/cpujan2020.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
			vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox.	
Oracle Security Updates	15-JAN-2020	**7.1 High**	**CVE-2020-2713** Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 14.1.0-14.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data.	https://www.oracle.com/security-alerts/cpujan2020.html
Oracle Security Updates	15-JAN-2020	**7.1 High**	**CVE-2020-2718** Vulnerability in the Oracle Banking Corporate Lending product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 12.3.0-12.4.0 and 14.0.0-14.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 7.1	https://www.oracle.com/security-alerts/cpujan2020.html
Oracle Security Updates	15-JAN-2020	**7.1 High**	**CVE-2020-2723** Vulnerability in the Oracle FLEXCUBE Investor Servicing product of Oracle Financial Services Applications	https://www.oracle.com/security-alerts/cpujan2020.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
			(component: Infrastructure). Supported versions that are affected are 12.1.0-12.4.0 and 14.0.0-14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data.	
Application: VMware				
VMware Security Advisories	15-JAN-2020	**7.8 High**	**CVE-2020-3941** The repair operation of VMware Tools for Windows 10.x.y has a race condition which may allow for privilege escalation in the Virtual Machine where Tools is installed. This vulnerability is not present in VMware Tools 11.x.y since the affected functionality is not present in VMware Tools 11.	https://www.vmware.com/security/advisories/VMSA-2020-0002.html
Application: Intel				
Intel Security Updates	14-DEC-2020	**6.5 Medium**	**CVE-2019-14600** Uncontrolled search path element in the installer for Intel(R) SNMP Subagent Stand-Alone for Windows* 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-00300.html
Intel Security Updates	14-JAN-2020	**6.3 Medium**	**CVE-2019-14615** Insufficient control flow in certain data structures for some Intel(R) Processors with Intel(R) Processor Graphics may allow an unauthenticated user to potentially enable information disclosure via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00314.html
Intel Security Updates	14-JAN-2020	**5.9 Medium**	**CVE-2019-14596** Improper access control in the installer for Intel(R) Chipset Device Software INF Utility before version 10.1.18 may	https://www.intel.com/content/www/us/en/security-

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
			allow an authenticated user to potentially enable denial of service via local access.	center/advisory/intel-sa-00306.html
Application: Wordpress				
Email Subscribers & Newsletters up to 4.3.0 on WordPress hash sql injection	08-JAN-2020	**9.8 CRITICAL**	**CVE-2019-20361** There was a flaw in the WordPress plugin, Email Subscribers & Newsletters before 4.3.1, that allowed SQL statements to be passed to the database in the hash parameter (a blind SQL injection vulnerability).	Upgrading to version 4.3.1.
Minimal Coming Soon & Maintenance Mode Plugin up to 2.10 on WordPress cross site request forgery	09-JAN-2020	**8.8 HIGH**	**CVE-2020-6167** A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.10, allows a CSRF attack to enable maintenance mode, inject XSS, modify several important settings, or include remote files as a logo.	https://wordpress.org/plugins/minimal-coming-soon-maintenance-mode/#developers
CityBook - WordPress Theme Vulnerability	13-JAN-2020	**7.5 HIGH**	**CVE-2019-20209** The CTHthemes CityBook before 2.3.4, TownHub before 1.0.6, and EasyBook before 1.2.2 themes for WordPress allow nsecure Direct Object Reference (IDOR) via wp-admin/admin-ajax.php to delete any page/post/listing.	-
CityBook WordPress Theme Vulnerability	13-JAN-2020	**6.1 HIGH**	**CVE-2019-20211** The CTHthemes CityBook before 2.3.4, TownHub before 1.0.6, and EasyBook before 1.2.2 themes for WordPress allow Persistent XSS via Listing Address, Listing Latitude, Listing Longitude, Email Address, Description, Name, Job or Position, Description, Service Name, Address, Latitude, Longitude, Phone Number, or Website.	-
Application: Google-Android				

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
Google – Android Security Updates	08-JAN-2020	**8.8 High**	**CVE-2020-0002** In ih264d_init_decoder of ih264d_api.c, there is a possible out of bounds write due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-142602711	https://source.android.com/security/bulletin/2020-01-01
Google – Android Security Updates	06-JAN-2020	**7.8 High**	**CVE-2019-9468** In export_key_der of export_key.cpp, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-139683471	https://source.android.com/security/bulletin/pixel/2019-12-01
Google – Android Security Updates	07-JAN-2020	**5.5 MEDIUM**	**CVE-2019-9465** In the Titan M handling of cryptographic operations, there is a possible information disclosure due to an unusual root cause. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-133258003	https://source.android.com/security/bulletin/pixel/2019-12-01
Application: Google-Chrome				
Google Chrome Security Updates	10-JAN-2020	**8.8 High**	**CVE-2020-6377** Use after free in audio in Google Chrome prior to 79.0.3945.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2020/01/stable-channel-update-for-desktop.html
Application: Mozilla				

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
Security vulnerabilities fixed in - Firefox 70	08-JAN-2020	**8.8 High**	**CVE-2019-11757** When following the value's prototype chain, it was possible to retain a reference to a locale, delete it, and subsequently reference it. This resulted in a use-after-free and a potentially exploitable crash. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.	https://www.mozilla.org/security/advisories/mfsa2019-33/ https://www.mozilla.org/security/advisories/mfsa2019-34/ https://www.mozilla.org/security/advisories/mfsa2019-35/
Application: Huawei				
Buffer Error Vulnerability in Some Huawei Products	03-JAN-2020	**7.5 High**	**CVE-2019-5304** Some Huawei products have a buffer error vulnerability. An unauthenticated, remote attacker could send specific MPLS Echo Request messages to the target products. Due to insufficient input validation of some parameters in the messages, successful exploit may cause the device to reset.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200102-01-buffer-en
Denial of Service Vulnerability in Several Smartphones	03-JAN-2020	**5.5 Medium**	**CVE-2020-1785** Mate 10 Pro;Honor V10;Honor 10;Nova 4 smartphones have a denial of service vulnerability. The system does not properly check the status of certain module during certain operations, an attacker should trick the user into installing a malicious application, successful exploit could cause reboot of the smartphone.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200102-03-smartphone-en
Application: Adobe				
Adobe Illustrator CC < 24.0.2 Multiple Vulnerabilites	17-JAN-2020	**9.8 Critical**	**CVE-2020-3710, CVE-2020-3711, CVE-2020-3712, CVE-2020-3713, CVE-2020-3714** The version of Adobe Illustrator CC on the remote Windows hosts is prior to 24.0.2. It is, therefore, affected multiple memory corruption vulnerabilities which could lead to arbitrary code execution on the remote host. An unauthenticated, local attacker could exploit these issues to execute arbitrary commands on the host.	Upgrade to Adobe Illustrator CC 24.0.2 or later. https://helpx.adobe.com/security/products/illustrator/apsb20-03.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
Adobe Experience Manager multiple vulnerabilities	15-JAN-2020	**7.5 High**	**CVE-2019-16467 CVE-2019-16468 CVE-2019-16469** Adobe Experience Manager versions 6.5, 6.4, 6.3, 6.2, 6.1, and 6.0 have an user interface injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	https://helpx.adobe.com/security/products/experience-manager/apsb20-01.html
Application: Cacti				
Cacti 1.2.8 data_sources.php header cross site scripting	15-JAN-2020	**6.1 Medium**	**CVE-2020-7106** Cacti 1.2.8 has stored XSS in data_sources.php, color_templates_item.php, graphs.php, graph_items.php, lib/api_automation.php, user_admin.php, and user_group_admin.php, as demonstrated by the description parameter in data_sources.php (a raw string from the database that is displayed by $header to trigger the XSS).	-

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