BGD e-GOV CIRT

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

Issue Date: 01-March-2020 **Issue Number:04**

Vulnerability	Publish Date	CSVV	CVE ID & Description	Patch
Application: Apache				
Apache Tomcat up to 7.0.99/8.5.50/9.0.30 AJP Connector Ghostcat privilege escalation	24-FEB-2020	9.8 CRITICAL	**CVE-2020-1938** When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to	Upgrading to version 7.0.100, 8.5.51 or 9.0.31 eliminates this vulnerability. https://lists.apache.org/thread.html/r75113652e46c4dee687236510649acfb70d2c63e074152049c3f399d@<notifications.ofbiz.apache.org> https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cnvd-2020-10487

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 Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.	
Jclouds scriptbuilder Statements class wrote a temporary file to a predictable location	18-FEB-2020	9.8 CRITICAL	**CVE-2014-4651** It was found that the jclouds scriptbuilder Statements class wrote a temporary file to a predictable location. An attacker could use this flaw to access sensitive data, cause a denial of service, or perform other attacks.	https://issues.apache.org/jira/browse/JCLOUDS-612
FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	10-FEB-2020	9.8 CRITICAL	**CVE-2020-8840** FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	https://github.com/FasterXML/jackson-databind/issues/2620 https://lists.apache.org/thread.html/r078e68a926ea6be12e8404e47f45aabf04bb4668e8265c0de41db6db@%3Ccommits.druid.apache.org%3E https://lists.debian.org/debian-lts-announce/2020/02/msg00020.html
Application: Microsoft				
Microsoft Excel Remote Code Execution Vulnerability	11-FEB-2020	8.8 HIGH	**CVE-2020-0759** 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-2020-0759

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 Data Sharing Service Elevation of Privilege Vulnerability	11-FEB-2020	7.8 HIGH	**CVE-2020-0747** **CVE-2020-0659** An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0659 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0747
Connected Devices Platform Service Elevation of Privilege Vulnerability	11-FEB-2020	7.8 HIGH	**CVE-2020-0740** **CVE-2020-0741** **CVE-2020-0742** **CVE-2020-0743** **CVE-2020-0749** **CVE-2020-0750** An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0740 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0741 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0742 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0743 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0749 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0750
Windows Error Reporting Elevation of Privilege Vulnerability	11-FEB-2020	7.8 HIGH	**CVE-2020-0753** **CVE-2020-0754** An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0753

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
			Reporting Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0754
Windows Graphics Component Elevation of Privilege Vulnerability	11-FEB-2020	7.8 HIGH	**CVE-2020-0792** **CVE-2020-0715** **CVE-2020-0745** 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-2020-0792 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0715 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0745
IPv6 Weakness Denial of Service Vulnerability	20-FEB-2020	7.5 HIGH	**CVE-2012-5364** The IPv6 implementation in Microsoft Windows 7 and earlier allows remote attackers to cause a denial of service via a flood of ICMPv6 Router Advertisement packets containing multiple Routing entries.	http://www.openwall.com/lists/oss-security/2012/10/10/12 https://www.securityfocus.com/bid/56170/info
Windows Hyper-V Denial of Service Vulnerability	11-FEB-2020	6.8 MEDIUM	**CVE-2020-0751** **CVE-2020-0661** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0751 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0661

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 Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	05-FEB-2020	9.8 CRITICAL	**CVE-2013-2681** Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	https://exchange.xforce.ibmcloud.com/vulnerabilities/84068 http://www.securityfocus.com/bid/59714
Cisco Smart Software Manager On-Prem Static Default Credential Vulnerability	19-FEB-2020	9.1 CRITICAL	**CVE-2020-3158** A vulnerability in the High Availability (HA) service of Cisco Smart Software Manager On-Prem could allow an unauthenticated, remote attacker to access a sensitive part of the system with a high-privileged account. The vulnerability is due to a system account that has a default and static password and is not under the control of the system administrator. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to obtain read and write access to system data, including the configuration of an affected device. The attacker would gain access to a sensitive portion of the system, but the attacker would not have full administrative rights to control the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-on-prem-static-cred-sL8rDs8
Cisco IP Phone Remote Code Execution and Denial of Service Vulnerability	05-FEB-2020	8.8 HIGH	**CVE-2020-3111** A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos

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
			with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	
Cisco Data Center Network Manager Cross-Site Request Forgery Vulnerability	19-FEB-2020	8.8 HIGH	**CVE-2020-3114** A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link while having an active session on an affected device. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200219-dcnm-csrf
Cisco ACE Log Retention Denial of Service Vulnerability	07-FEB-2020	7.5 HIGH	**CVE-2013-1202** Cisco ACE A2(3.6) allows log retention DoS.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20130516-CVE-2013-1202
Cisco Enterprise NFV Infrastructure Software Remote Code Execution Vulnerability	19-FEB-2020	6.7 MEDIUM	**CVE-2020-3138** A vulnerability in the upgrade component of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to install a malicious file when upgrading. The vulnerability is due to insufficient signature validation. An attacker could exploit this vulnerability by providing a crafted upgrade file. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-codex-shs4NhvS

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 to upload crafted code to the affected device.	
Application: Adobe				
Adobe Framemaker up to 2019.0.4 Code Execution memory corruption	13-FEB-2020	9.8 CRITICAL	**CVE-2020-3734** **CVE-2020-3731** **CVE-2020-3735** Adobe Framemaker versions 2019.0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html
Application: IBM				
Multiple buffer overflow vulnerabilities exist in IBM® Db2® leading to privilege escalation.	19-FEB-2020	7.8 HIGH	**CVE-2020-4204** IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 174960.	https://www.ibm.com/support/pages/node/2875875 https://exchange.xforce.ibmcloud.com/vulnerabilities/174960
IBM Db2 is vulnerable to denial of service	19-FEB-2020	7.5 HIGH	**CVE-2020-4135** IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated user to send specially crafted packets to cause a denial of service from excessive memory usage.	https://www.ibm.com/support/pages/node/2876307 https://exchange.xforce.ibmcloud.com/vulnerabilities/173806
Application: Huawei				
Command Injection Vulnerability in GaussDB 200	17-FEB-2020	8.8 HIGH	**CVE-2020-1790** GaussDB 200 with version of 6.5.1 have a command injection vulnerability. The software constructs part of a command using external input from users, but the software does not sufficiently validate the user input. Successful exploit could allow the attacker to inject certain commands.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-gauss-en
Command Injection Vulnerability in GaussDB 200 Product	17-FEB-2020	8.5 HIGH	**CVE-2020-1811** GaussDB 200 with version of 6.5.1 have a command injection vulnerability. Due to insufficient input validation, remote	https://www.huawei.com/en/psirt/security-advisories/huawei-

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
			attackers with low permissions could exploit this vulnerability by sending crafted commands to the affected device. Successful exploit could allow an attacker to execute commands.	sa-20200120-01-gaussdb200-en
Improper Authentication Vulnerability in Smartphones	17-FEB-2020	7.8 HIGH	**CVE-2020-1812** HUAWEI P30 smartphones with versions earlier than 10.0.0.173(C00E73R1P11) have an improper authentication vulnerability. Due to improperly validation of certain application, an attacker should trick the user into installing a malicious application to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-smartphone-en
Information Leak Vulnerability in Some Huawei Products	17-FEB-2020	7.5 HIGH	**CVE-2020-1841** Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en
Memory Leak Vulnerability in Some Firewall Products	17-FEB-2020	7.5 HIGH	**CVE-2020-1815** Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-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
			memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust.	
Huawei NIP6800	17-FEB-2020	7.5 HIGH	**CVE-2020-1815** Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en
Denial of Service Vulnerability in Some Huawei Firewall Products	17-FEB-2020	7.5 HIGH	**CVE-2020-1816** Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPSec function of the affected device abnormal.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en
Application: Google				
Google – Chrome Security Updates	17-FEB-2020	8.8 HIGH	**11-FEB-2020** Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://crbug.com/1042254 https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop.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
Google – Android Security Updates	13-FEB-2020	8.8 HIGH	**CVE-2020-0022** In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143894715	https://source.android.com/security/bulletin/2020-02-01
Google – Android Security Updates	20-FEB-2020	8.1 HIGH	**CVE-2014-7914** btif/src/btif_dm.c in Android before 5.1 does not properly enforce the temporary nature of a Bluetooth pairing, which allows user-assisted remote attackers to bypass intended access restrictions via crafted Bluetooth packets after the tapping of a crafted NFC tag.	https://android.googlesource.com/platform/external/bluetooth/bluedroid/+/0360aa7c418152a3e5e335a065ac3629cbb09559
Google – Android Security Updates	13-FEB-2020	7.8 HIGH	**CVE-2020-0026** In Parcel::continueWrite of Parcel.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-140419401	https://source.android.com/security/bulletin/2020-02-01
Google – Android Security Updates	13-FEB-2020	7.8 HIGH	**CVE-2020-0027** In HidRawSensor::batch of HidRawSensor.cpp, there is a possible out of bounds write due to an unexpected switch fallthrough. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144040966	https://source.android.com/security/bulletin/2020-02-01

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	13-FEB-2020	7.0 HIGH	**CVE-2020-0030** In binder_thread_release of binder.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-145286050References: Upstream kernel	https://source.android.com/security/bulletin/2020-02-01
Application: MOVEit Transfer				
Vulnerabilities in Progress MOVEit Transfer	14-FEB-2020	8.8 HIGH	**CVE-2020-8611:** In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements.	https://community.ipswitch.com/s/article/MOVEit-Transfer-Security-Vulnerabilities-Feb-2020 https://docs.ipswitch.com/MOVEit/Transfer2019_1/ReleaseNotes/en/index.htm#49443.htm https://docs.ipswitch.com/MOVEit/Transfer2019_2/ReleaseNotes/en/index.htm#49677.htm
Application: Aircrack-ng				
Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	31-JAN-2020	9.8 CRITICAL	**CVE-2014-8322** Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	https://github.com/aircrack-ng/aircrack-ng/pull/14 http://aircrack-ng.blogspot.com/2014/10/aircrack-ng-12-release-candidate-1.html https://github.com/aircrack-ng/aircrack-ng/commit/091b153f294b9b695b0b2831e65936438b550d7b

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
				http://packetstormsecurity.com/files/128943/Aircrack-ng-1.2-Beta-3-DoS-Code-Execution.html
Application: Netgear				
NETGEAR AC1200 R6220 Firmware vulnerability	10-FEB-2020	9.4 CRITICAL	**CVE-2019-17137** This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR AC1200 R6220 Firmware version 1.1.0.86 Smart WiFi Router. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of path strings. By inserting a null byte into the path, the user can skip most authentication checks. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-8616.	-
Application: Qualcomn				
Qualcomm Security update	07-FEB-2020	9.1 CRITICAL	**CVE-2019-14057** Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/february-2020-bulletin -

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
			SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	
Application: Squid				
Squid Security update	04-FEB-2020	7.3 HIGH	**CVE-2020-8450** An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	http://www.squid-cache.org/Advisories/SQUID-2020_1.txt http://www.squid-cache.org/Versions/v4/changesets/squid-4-d8e4715992d0e530871519549add5519cbac0598.patch
Application: Wordpress				
wpCentral security update	17-FEB-2020	8.8 HIGH	**CVE-2020-9043** The wpCentral plugin before 1.5.1 for WordPress allows disclosure of the connection key.	https://wordpress.org/plugins/wp-central/#developers https://plugins.trac.wordpress.org/changeset?&old=2244363%40wp-central&new=2244363%40wp-central
Application: Zabbix				
Zabbix Security update	17-FEB-2020	9.8 CRITICAL	**CVE-2013-3738** A File Inclusion vulnerability exists in Zabbix 2.0.6 due to inadequate sanitization of request strings in CGI scripts, which could let a remote malicious user execute arbitrary code.	http://support.zabbix.com/browse/ZBX-6652
Application: Zend				
Zend Framework Security update	11-FEB-2020	9.8 CRITICAL	**CVE-2014-2052** Zend Framework, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	https://owncloud.org/security/advisories/xxe-multiple-third-party-components/ http://owncloud.org/about/security/advisories/oC-SA-2014-006/

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