National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Jan 2020 Vol. 07 No. 01

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
appspace					
on-prem					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-01-2020	4.3	In Appspace On-Prem through 7.1.3, an adversary can steal a session token via XSS. **CVE ID : CVE-2020-5393**	https://docs.appspace.com/latest/release-notes/7-1-platform-release-notes/#Patch_Updates	A-APP-ON-P-160120/1
Codoforum					
codoforum					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-01-2020	3.5	Codoforum 4.8.3 allows XSS in the admin dashboard via a name field of a new user, i.e., on the Manage Users screen. **CVE ID : CVE-2020-5305**	N/A	A-COD-CODO-160120/2
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-01-2020	3.5	Codoforum 4.8.3 allows XSS via a post using parameters display name, title name, or content. **CVE ID : CVE-2020-5306**	N/A	A-COD-CODO-160120/3
Improper Neutralization of Input During Web	07-01-2020	4.3	Codoforum 4.8.3 allows XSS in the user registration page: via the username field to the index.php?u=/user/register	N/A	A-COD-CODO-160120/4

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			URI. The payload is, for example, executed on the admin/index.php?page=users/manage page. **CVE ID : CVE-2020-5842**		
Codologic					
codoforum					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-01-2020	3.5	Codoforum 4.8.3 allows XSS in the admin dashboard via a category to the Manage Users screen. **CVE ID : CVE-2020-5843**	N/A	A-COD-CODO-160120/5
fontforge					
fontforge					
Use After Free	03-01-2020	6.8	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c. **CVE ID : CVE-2020-5395**	N/A	A-FON-FONT-160120/6
Out-of-bounds Write	03-01-2020	6.8	FontForge 20190801 has a heap-based buffer overflow in the Type2NotDefSplines() function in splinesave.c. **CVE ID : CVE-2020-5496**	N/A	A-FON-FONT-160120/7
Ftpgetter					
ftpgetter					
NULL Pointer Dereference	08-01-2020	5	FTPGetter Professional 5.97.0.223 is vulnerable to a memory corruption bug when a user sends a specially crafted string to the application. This memory corruption bug can possibly be classified as a NULL	N/A	A-FTP-FTPG-160120/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference. **CVE ID : CVE-2020-5183**		
gilacms					
gila_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-01-2020	6.8	Gila CMS 1.11.8 allows /admin/media?path=../ Path Traversal. **CVE ID : CVE-2020-5512**	N/A	A-GIL-GILA-160120/9
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-01-2020	6.8	Gila CMS 1.11.8 allows /cm/delete?t=../ Directory Traversal. **CVE ID : CVE-2020-5513**	N/A	A-GIL-GILA-160120/10
Unrestricted Upload of File with Dangerous Type	06-01-2020	9	Gila CMS 1.11.8 allows Unrestricted Upload of a File with a Dangerous Type via .phar or .phtml to the lzld/thumb?src= URI. **CVE ID : CVE-2020-5514**	N/A	A-GIL-GILA-160120/11
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-01-2020	6.5	Gila CMS 1.11.8 allows /admin/sql?query= SQL Injection. **CVE ID : CVE-2020-5515**	N/A	A-GIL-GILA-160120/12
GNU					
libredwg					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-01-2020	6.8	GNU LibreDWG 0.9.3.2564 has a heap-based buffer over-read in read_pages_map in decode_r2007.c. **CVE ID : CVE-2020-6609**	N/A	A-GNU-LIBR-160120/13
Uncontrolled Resource Consumption	08-01-2020	4.3	GNU LibreDWG 0.9.3.2564 has an attempted excessive memory allocation in read_sections_map in decode_r2007.c. **CVE ID : CVE-2020-6610**	N/A	A-GNU-LIBR-160120/14
NULL Pointer Dereference	08-01-2020	4.3	GNU LibreDWG 0.9.3.2564 has a NULL pointer dereference in get_next_owned_entity in dwg.c. **CVE ID : CVE-2020-6611**	N/A	A-GNU-LIBR-160120/15
Out-of-bounds Read	08-01-2020	5.8	GNU LibreDWG 0.9.3.2564 has a heap-based buffer over-read in copy_compressed_bytes in decode_r2007.c. **CVE ID : CVE-2020-6612**	N/A	A-GNU-LIBR-160120/16
Out-of-bounds Read	08-01-2020	5.8	GNU LibreDWG 0.9.3.2564 has a heap-based buffer over-read in bit_search_sentinel in bits.c. **CVE ID : CVE-2020-6613**	N/A	A-GNU-LIBR-160120/17
Out-of-bounds Read	08-01-2020	5.8	GNU LibreDWG 0.9.3.2564 has a heap-based buffer over-read in bfr_read in decode.c. **CVE ID : CVE-2020-6614**	N/A	A-GNU-LIBR-160120/18
NULL Pointer Dereference	08-01-2020	4.3	GNU LibreDWG 0.9.3.2564 has an invalid pointer dereference in	N/A	A-GNU-LIBR-160120/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dwg_dynapi_entity_value in dynapi.c (dynapi.c is generated by gen-dynapi.pl). **CVE ID : CVE-2020-6615**		
gpac					
gpac					
NULL Pointer Dereference	09-01-2020	4.3	An issue was discovered in GPAC version 0.8.0. There is a NULL pointer dereference in the function gf_isom_get_media_data_size() in isomedia/isom_read.c. **CVE ID : CVE-2020-6630**	N/A	A-GPA-GPAC-160120/20
NULL Pointer Dereference	09-01-2020	4.3	An issue was discovered in GPAC version 0.8.0. There is a NULL pointer dereference in the function gf_m2ts_stream_process_pmt() in media_tools/m2ts_mux.c. **CVE ID : CVE-2020-6631**	N/A	A-GPA-GPAC-160120/21
hashbrowncms					
hashbrown_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-01-2020	5	An issue was discovered in HashBrown CMS before 1.3.2. Server/Entity/Resource/Connection.js allows an attacker to reach a parent directory via a crafted name or ID field. **CVE ID : CVE-2020-5840**	N/A	A-HAS-HASH-160120/22
mitreid					
connect					
Improper Neutralization of Input	04-01-2020	4.3	The OpenID Connect reference implementation for MITREid Connect	N/A	A-MIT-CONN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			through 1.3.3 allows XSS due to userInfoJson being included in the page unsanitized. This is related to header.tag. The issue can be exploited to execute arbitrary JavaScript. **CVE ID : CVE-2020-5497**		160120/23
mruby					
mruby					
Use After Free	11-01-2020	7.5	In mruby 2.1.0, there is a use-after-free in hash_values_at in mrbgems/mruby-hash-ext/src/hash-ext.c. **CVE ID : CVE-2020-6838**	N/A	A-MRU-MRUB-160120/24
Out-of-bounds Write	11-01-2020	7.5	In mruby 2.1.0, there is a stack-based buffer overflow in mrb_str_len_to_dbl in string.c. **CVE ID : CVE-2020-6839**	N/A	A-MRU-MRUB-160120/25
Use After Free	11-01-2020	7.5	In mruby 2.1.0, there is a use-after-free in hash_slice in mrbgems/mruby-hash-ext/src/hash-ext.c. **CVE ID : CVE-2020-6840**	N/A	A-MRU-MRUB-160120/26
nothings					
stb_truetype.h					
Reachable Assertion	08-01-2020	6.8	stb stb_truetype.h through 1.22 has an assertion failure in stbtt__cff_int. **CVE ID : CVE-2020-6617**	N/A	A-NOT-STB_-160120/27
Out-of-bounds Read	08-01-2020	6.8	stb stb_truetype.h through 1.22 has a heap-based buffer over-read in stbtt__find_table.	N/A	A-NOT-STB_-160120/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6618		
Reachable Assertion	08-01-2020	6.8	stb stb_truetype.h through 1.22 has an assertion failure in stbtt__buf_seek. **CVE ID : CVE-2020-6619**	N/A	A-NOT-STB_-160120/29
Out-of-bounds Read	08-01-2020	6.8	stb stb_truetype.h through 1.22 has a heap-based buffer over-read in stbtt__buf_get8. **CVE ID : CVE-2020-6620**	N/A	A-NOT-STB_-160120/30
Out-of-bounds Read	08-01-2020	6.8	stb stb_truetype.h through 1.22 has a heap-based buffer over-read in ttUSHORT. **CVE ID : CVE-2020-6621**	N/A	A-NOT-STB_-160120/31
Out-of-bounds Read	08-01-2020	6.8	stb stb_truetype.h through 1.22 has a heap-based buffer over-read in stbtt__buf_peek8. **CVE ID : CVE-2020-6622**	N/A	A-NOT-STB_-160120/32
Reachable Assertion	08-01-2020	6.8	stb stb_truetype.h through 1.22 has an assertion failure in stbtt__cff_get_index. **CVE ID : CVE-2020-6623**	N/A	A-NOT-STB_-160120/33
Openjpeg					
openjpeg					
Out-of-bounds Write	13-01-2020	5	OpenJPEG through 2.3.1 has a heap-based buffer overflow in opj_t1_clbl_decode_processor in libopenjp2.so. **CVE ID : CVE-2020-6851**	N/A	A-OPE-OPEN-160120/34
phpgurukul					
hospital_management_system_in_php					
Improper Neutralization of Input During Web	06-01-2020	4.3	PHPGurukul Hospital Management System in PHP v4.0 suffers from multiple Persistent XSS	N/A	A-PHP-HOSP-160120/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			vulnerabilities. **CVE ID : CVE-2020-5191**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-01-2020	6.5	PHPGurukul Hospital Management System in PHP v4.0 suffers from multiple SQL injection vulnerabilities: multiple pages and parameters are not validating user input, and allow for the application's database and information to be fully compromised. **CVE ID : CVE-2020-5192**	N/A	A-PHP-HOSP-160120/36
hostel_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-01-2020	10	PHPGurukul Hostel Management System v2.0 allows SQL injection via the id parameter in the full-profile.php file. **CVE ID : CVE-2020-5510**	N/A	A-PHP-HOST-160120/37
Python					
pillow					
Integer Overflow or Wraparound	03-01-2020	6.8	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc. **CVE ID : CVE-2020-5310**	N/A	A-PYT-PILL-160120/38
Buffer Copy without Checking Size of Input ('Classic Buffer	03-01-2020	6.8	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow. **CVE ID : CVE-2020-5311**	N/A	A-PYT-PILL-160120/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-01-2020	6.8	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow. **CVE ID : CVE-2020-5312**	N/A	A-PYT-PILL-160120/40
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-01-2020	6.8	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow. **CVE ID : CVE-2020-5313**	N/A	A-PYT-PILL-160120/41
Troglobit					
uftpd					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-01-2020	6.5	In uftpd before 2.11, there is a buffer overflow vulnerability in handle_PORT in ftpcmd.c that is caused by a buffer that is 16 bytes large being filled via sprintf() with user input based on the format specifier string %d.%d.%d.%d. The 16 byte size is correct for valid IPv4 addresses (len('255.255.255.255 ') == 16), but the format specifier %d allows more than 3 digits. This has been fixed in version 2.11 **CVE ID : CVE-2020-5204**	https://github.com/troglobit/uftpd/security/advisories/GHSA-wrpr-xw7q-9wvq	A-TRO-UFTP-160120/42
webfactoryltd					
minimal_coming_soon_\&_maintenance_mode					
Incorrect	09-01-2020	5.5	A flaw in the WordPress	https://word	A-WEB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			plugin, Minimal Coming Soon & Maintenance Mode through 2.15, allows authenticated users with basic access to export settings and change maintenance-mode themes. **CVE ID : CVE-2020-6166**	press.org/plugins/minimal-coming-soon-maintenance-mode/#developers	MINI-160120/43
Cross-Site Request Forgery (CSRF)	09-01-2020	6.8	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. **CVE ID : CVE-2020-6167**	https://wordpress.org/plugins/minimal-coming-soon-maintenance-mode/#developers	A-WEB-MINI-160120/44
Incorrect Permission Assignment for Critical Resource	09-01-2020	6.5	A flaw in the WordPress plugin, Minimal Coming Soon & Maintenance Mode through 2.10, allows authenticated users with basic access to enable and disable maintenance-mode settings (impacting the availability and confidentiality of a vulnerable site, along with the integrity of the setting). **CVE ID : CVE-2020-6168**	https://wordpress.org/plugins/minimal-coming-soon-maintenance-mode/#developers	A-WEB-MINI-160120/45
Operating System					
comtechtel					
stampede_fx-1010_firmware					
Improper Neutralization of Special	02-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated	N/A	O-COM-STAM-160120/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			administrators to execute arbitrary OS commands by navigating to the Diagnostics Ping page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-5179**		
Google					
android					
Improper Privilege Management	08-01-2020	7.2	In getProcessRecordLocked of ActivityManagerService.java isolated apps are not handled correctly. 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-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-140055304 **CVE ID : CVE-2020-0001**	https://source.android.com/security/bulletin/2020-01-01	O-GOO-ANDR-160120/47
Use After Free	08-01-2020	9.3	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,	https://source.android.com/security/bulletin/2020-01-04	O-GOO-ANDR-160120/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Android-10 Android ID: A-142602711 **CVE ID : CVE-2020-0002**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-01-2020	3.7	In onCreate of InstallStart.java, there is a possible package validation bypass due to a time-of-check time-of-use vulnerability. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-8.0 Android ID: A-140195904 **CVE ID : CVE-2020-0003**	https://source.android.com/security/bulletin/2020-01-02	O-GOO-ANDR-160120/49
Improper Input Validation	08-01-2020	2.1	In generateCrop of WallpaperManagerService.java, there is a possible sysui crash due to image exceeding maximum texture size. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-120847476 **CVE ID : CVE-2020-0004**	https://source.android.com/security/bulletin/2020-01-03	O-GOO-ANDR-160120/50
N/A	08-01-2020	4.3	In rw_i93_send_cmd_write_single_block of rw_i93.cc, there is a possible information disclosure of heap memory	https://source.android.com/security/bulletin/2020-01-05	O-GOO-ANDR-160120/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to uninitialized data. This could lead to remote information disclosure in the NFC server 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-139738828 **CVE ID : CVE-2020-0006**		
N/A	08-01-2020	2.1	In flattenString8 of Sensor.cpp, there is a possible information disclosure of heap memory due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-141890807 **CVE ID : CVE-2020-0007**	https://source.android.com/security/bulletin/2020-01-06	O-GOO-ANDR-160120/52
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-01-2020	1.9	In LowEnergyClient::MtuChangedCallback of low_energy_client.cc, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2020-01-07	O-GOO-ANDR-160120/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Product: Android Versions: Android-8.0, Android-8.1, Android-9, and Android-10 Android ID: A-142558228 **CVE ID : CVE-2020-0008**		
Incorrect Default Permissions	08-01-2020	2.1	In calc_vm_may_flags of ashmem.c, there is a possible arbitrary write to shared memory due to a permissions bypass. This could lead to local escalation of privilege by corrupting memory shared between processes, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-142938932 **CVE ID : CVE-2020-0009**	https://source.android.com/security/bulletin/2020-01-11	O-GOO-ANDR-160120/54
Huawei					
honor_v10_firmware					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	O-HUA-HONO-160120/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mate_10_pro_firmware					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	O-HUA-MATE-160120/56
nova_4_firmware					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	O-HUA-NOVA-160120/57
honor_10_firmware					
Improper Input Validation	03-01-2020	7.1	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	N/A	O-HUA-HONO-160120/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			should trick the user into installing a malicious application, successful exploit could cause reboot of the smartphone. **CVE ID : CVE-2020-1785**		
usg9500_firmware					
Insufficiently Protected Credentials	03-01-2020	6.4	USG9500 with software of V500R001C30SPC100; V500R001C30SPC200; V500R001C30SPC600; V500R001C60SPC500; V500R005C00SPC100; V500R005C00SPC200 have an improper credentials management vulnerability. The software does not properly manage certain credentials. Successful exploit could cause information disclosure or damage, and impact the confidentiality or integrity. **CVE ID : CVE-2020-1871**	N/A	O-HUA-USG9-160120/59
Hardware					
comtechtel					
stampede_fx-1010					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Diagnostics Ping page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech	N/A	H-COM-STAM-160120/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account.) **CVE ID : CVE-2020-5179**		
Huawei					
honor_v10					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	H-HUA-HONO-160120/61
mate_10_pro					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	H-HUA-MATE-160120/62
honor_10					
Improper Input Validation	03-01-2020	7.1	Mate 10 Pro;Honor V10;Honor 10;Nova 4 smartphones have a denial of service vulnerability. The	N/A	H-HUA-HONO-160120/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-1785**		
nova_4					
Improper Input Validation	03-01-2020	7.1	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. **CVE ID : CVE-2020-1785**	N/A	H-HUA-NOVA-160120/64
usg9500					
Insufficiently Protected Credentials	03-01-2020	6.4	USG9500 with software of V500R001C30SPC100; V500R001C30SPC200; V500R001C30SPC600; V500R001C60SPC500; V500R005C00SPC100; V500R005C00SPC200 have an improper credentials management vulnerability. The software does not properly manage certain credentials. Successful exploit could cause	N/A	H-HUA-USG9-160120/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure or damage, and impact the confidentiality or integrity. **CVE ID : CVE-2020-1871**		