Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
accessally					
accessally					
Exposure of Sensitive Information to an Unauthorized Actor	12-04-2021	5	In the AccessAlly WordPress plugin before 3.5.7, the file "resource/frontend/product/product-shortcode.php" responsible for the [accessally_order_form] shortcode is dumping serialize($_SERVER), which contains all environment variables. The leakage occurs on all public facing pages containing the [accessally_order_form] shortcode, no login or administrator role is required. **CVE ID : CVE-2021-24226**	https://wpscan.com/vulnerability/8e3e89fd-e380-4108-be23-00e87fbaad16	A-ACC-ACCE-280421/1
adobe					
acrobat					
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28545**		
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/3
acrobat_dc					
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the certification. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28545**		
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/5
acrobat_reader					
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. **CVE ID : CVE-2021-28545**		
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/7
acrobat_reader_dc					
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28545**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-280421/9
bridge					
Improper Authorization	15-04-2021	2.1	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Improper Authorization vulnerability in the Genuine Software Service. A low-privileged attacker could leverage this vulnerability to achieve application denial-of-service in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2021-21096**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/10
Out-of-bounds Write	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds write vulnerability when parsing a crafted file. An unauthenticated	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21095**		
Out-of-bounds Write	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21094**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/12
Access of Memory Location After End of Buffer	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21093		
Access of Memory Location After End of Buffer	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21092**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/14
Out-of-bounds Read	15-04-2021	4.3	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21091**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	A-ADO-BRID-280421/15
coldfusion					
Improper Neutralization of Input During Web Page Generation	15-04-2021	6	Adobe Coldfusion versions 2016 (update 16 and earlier), 2018 (update 10 and earlier) and 2021.0.0.323925 are affected by an Improper	https://helpx.adobe.com/security/products/coldfusion/apsb2	A-ADO-COLD-280421/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') vulnerability. An attacker could abuse this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction. **CVE ID : CVE-2021-21087**	1-16.html	
digital_editions					
Creation of Temporary File in Directory with Insecure Permissions	15-04-2021	6.8	Adobe Digital Editions version 4.5.11.187245 (and earlier) is affected by a Privilege Escalation vulnerability during installation. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary file system write in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21100**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-26.html	A-ADO-DIGI-280421/17
photoshop					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-04-2021	6.8	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/photoshop/apsb21-28.html	A-ADO-PHOT-280421/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28548**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-04-2021	6.8	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28549**	https://helpx.adobe.com/security/products/photoshop/apsb21-28.html	A-ADO-PHOT-280421/19
adtensor_project					
adtensor					
Use of Uninitialized Resource	01-04-2021	7.5	An issue was discovered in the adtensor crate through 2021-01-11 for Rust. There is a drop of uninitialized memory via the FromIterator implementation for Vector and Matrix. **CVE ID : CVE-2021-29936**	https://rustsec.org/advisories/RUSTSEC-2021-0045.html	A-ADT-ADTE-280421/20
algolplus					
advanced_order_export					
Improper Neutralization of Input During Web Page Generation	05-04-2021	4.3	This Advanced Order Export For WooCommerce WordPress plugin before 3.1.8 helps you to easily export WooCommerce order data. The tab	https://wpscan.com/vulnerability/09681a6c-57b8-4448-	A-ALG-ADVA-280421/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			parameter in the Admin Panel is vulnerable to reflected XSS. **CVE ID : CVE-2021-24169**	982a-fe8d28c87fc3	
altn					
mdaemon					
Externally Controlled Reference to a Resource in Another Sphere	14-04-2021	6.5	An issue was discovered in MDaemon before 20.0.4. Administrators can use Remote Administration to exploit an Arbitrary File Write vulnerability. An attacker is able to create new files in any location of the filesystem, or he may be able to modify existing files. This vulnerability may directly lead to Remote Code Execution. **CVE ID : CVE-2021-27183**	https://www.altn.com/Support/SecurityUpdate/MD011221_MDaemon_EN/	A-ALT-MDAE-280421/22
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-04-2021	6.5	An issue was discovered in MDaemon before 20.0.4. There is an IFRAME injection vulnerability in Webmail (aka WorldClient). It can be exploited via an email message. It allows an attacker to perform any action with the privileges of the attacked user. **CVE ID : CVE-2021-27182**	https://www.altn.com/Support/SecurityUpdate/MD011221_MDaemon_EN/	A-ALT-MDAE-280421/23
Cross-Site Request Forgery (CSRF)	14-04-2021	6.8	An issue was discovered in MDaemon before 20.0.4. Remote Administration allows an attacker to perform a fixation of the anti-CSRF token. In order to exploit this issue, the user has to click on a malicious URL provided by	https://www.altn.com/Support/SecurityUpdate/MD011221_MDaemon_EN/	A-ALT-MDAE-280421/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker and successfully authenticate into the application. Having the value of the anti-CSRF token, the attacker may trick the user into visiting his malicious page and performing any request with the privileges of attacked user. **CVE ID : CVE-2021-27181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2021	4.3	An issue was discovered in MDaemon before 20.0.4. There is Reflected XSS in Webmail (aka WorldClient). It can be exploited via a GET request. It allows performing any action with the privileges of the attacked user. **CVE ID : CVE-2021-27180**	https://www.altn.com/Support/SecurityUpdate/MD011221_MDaemon_EN/	A-ALT-MDAE-280421/25
ampache					
ampache					
Improper Access Control	13-04-2021	5	Ampache is a web based audio/video streaming application and file manager. Versions prior to 4.4.1 allow unauthenticated access to Ampache using the subsonic API. To successfully make the attack you must use a username that is not part of the site to bypass the auth checks. For more details and workaround guidance see the referenced GitHub security advisory. **CVE ID : CVE-2021-21399**	https://github.com/ampache/ampache/security/advisories/GHSA-p9pm-j95j-5mjf	A-AMP-AMPA-280421/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apache					
commons_io					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2021	5	In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value. **CVE ID : CVE-2021-29425**	https://issues.apache.org/jira/browse/IO-556, https://lists.apache.org/thread.html/rc359823b5500e9a9a2572678ddb8e01d3505a7ffcadfa8d13b8780ab%40%3Cuser.commons.apache.org%3E	A-APA-COMM-280421/27
cxf					
Uncontrolled Resource Consumption	02-04-2021	5	CXF supports (via JwtRequestCodeFilter) passing OAuth 2 parameters via a JWT token as opposed to query parameters (see: The OAuth 2.0 Authorization Framework: JWT Secured Authorization Request (JAR)). Instead of sending a JWT token as a "request" parameter, the spec also supports specifying a URI from which to retrieve a JWT token from via the "request_uri" parameter. CXF was not validating the "request_uri" parameter (apart from ensuring it uses "https) and was	https://cxf.apache.org/security-advisories.data/CVE-2021-22696.txt.asc, https://lists.apache.org/thread.html/r8651c06212c56294a1c0ea61a5ad7790c06502209c03f05c0c7c9914@	A-APA-CXF-280421/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			making a REST request to the parameter in the request to retrieve a token. This means that CXF was vulnerable to DDos attacks on the authorization server, as specified in section 10.4.1 of the spec. This issue affects Apache CXF versions prior to 3.4.3; Apache CXF versions prior to 3.3.10. **CVE ID : CVE-2021-22696**	%3Cusers.cxf.apache.org%3E	
solr					
Incorrect Authorization	13-04-2021	6.4	When using ConfigurableInternodeAuthHadoopPlugin for authentication, Apache Solr versions prior to 8.8.2 would forward/proxy distributed requests using server credentials instead of original client credentials. This would result in incorrect authorization resolution on the receiving hosts. **CVE ID : CVE-2021-29943**	https://lists.apache.org/thread.html/r91dd0ff556e0c9aab4c92852e0e540c59d4633718ce12881558cf44d%40%3Cusers.solr.apache.org%3E	A-APA-SOLR-280421/29
Insufficiently Protected Credentials	13-04-2021	4.3	When starting Apache Solr versions prior to 8.8.2, configured with the SaslZkACLProvider or VMParamsAllAndReadonlyDigestZkACLProvider and no existing security.json znode, if the optional read-only user is configured then Solr would not treat that node as a sensitive path and would allow it to be readable. Additionally, with any ZkACLProvider, if	https://lists.apache.org/thread.html/r536da4c4e4e406f7843461cc754a3d0a3fe575aa576e2b71a9cd57d0%40%3Cannounce.apache.org%3	A-APA-SOLR-280421/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the security.json is already present, Solr will not automatically update the ACLs. **CVE ID : CVE-2021-29262**	E	
apple					
safari					
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	A-APP-SAFA-280421/31
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223,	A-APP-SAFA-280421/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2021-1844**	https://support.apple.com/en-us/HT212220, https://support.apple.com/en-us/HT212221	
xcode					
N/A	02-04-2021	4.3	A path handling issue was addressed with improved validation. This issue is fixed in Xcode 12.4. A malicious application may be able to access arbitrary files on the host device while running an app that uses on-demand resources with Xcode. **CVE ID : CVE-2021-1800**	https://support.apple.com/en-us/HT212153	A-APP-XCOD-280421/33
appspace					
appspace					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2021	3.5	Appspace 6.2.4 is vulnerable to stored cross-site scripting (XSS) in multiple parameters within /medianet/sgcontentset.aspx. **CVE ID : CVE-2021-27989**	N/A	A-APP-APPS-280421/34
Improper Authentication	14-04-2021	5	Appspace 6.2.4 is vulnerable to a broken authentication mechanism where pages such as /medianet/mail.aspx can be called directly and the framework is exposed with layouts, menus and functionalities.	http://appspace.com	A-APP-APPS-280421/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27990		
aprelium					
abyss_web_server_x1					
Out-of-bounds Read	08-04-2021	5	An issue was discovered in Aprelium Abyss Web Server X1 2.12.1 and 2.14. A crafted HTTP request can lead to an out-of-bounds read that crashes the application. **CVE ID : CVE-2021-3328**	N/A	A-APR-ABYS-280421/36
arenavec_project					
arenavec					
Out-of-bounds Write	01-04-2021	5	An issue was discovered in the arenavec crate through 2021-01-12 for Rust. A drop of uninitialized memory can sometimes occur upon a panic in T::default(). **CVE ID : CVE-2021-29930**	https://rustsec.org/advisories/RUSTSEC-2021-0040.html	A-ARE-AREN-280421/37
Double Free	01-04-2021	5	An issue was discovered in the arenavec crate through 2021-01-12 for Rust. A double drop can sometimes occur upon a panic in T::drop(). **CVE ID : CVE-2021-29931**	https://rustsec.org/advisories/RUSTSEC-2021-0040.html	A-ARE-AREN-280421/38
asus					
gputweak_ii					
Improper Privilege Management	08-04-2021	7.2	AsIO2_64.sys and AsIO2_32.sys in ASUS GPUTweak II before 2.3.0.3 allow low-privileged users to interact directly with physical memory (by calling one of several driver routines that map physical memory into the virtual	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/	A-ASU-GPUT-280421/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address space of the calling process) and to interact with MSR registers. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl. **CVE ID : CVE-2021-28685**		
Out-of-bounds Write	08-04-2021	2.1	AsIO2_64.sys and AsIO2_32.sys in ASUS GPUTweak II before 2.3.0.3 allow low-privileged users to trigger a stack-based buffer overflow. This could enable low-privileged users to achieve Denial of Service via a DeviceIoControl. **CVE ID : CVE-2021-28686**	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/	A-ASU-GPUT-280421/40
atlassian					
confluence					
Server-Side Request Forgery (SSRF)	01-04-2021	4	The WidgetConnector plugin in Confluence Server and Confluence Data Center before version 5.8.6 allowed remote attackers to manipulate the content of internal network resources via a blind Server-Side Request Forgery (SSRF) vulnerability. **CVE ID : CVE-2021-26072**	https://jira.atlassian.com/browse/CONFSERVER-61399	A-ATL-CONF-280421/41
data_center					
Cross-Site Request Forgery (CSRF)	01-04-2021	3.5	The SetFeatureEnabled.jspa resource in Jira Server and Data Center before version 8.5.13, from version 8.6.0 before version 8.13.5, and from version 8.14.0 before	https://jira.atlassian.com/browse/JRASERVER-72233	A-ATL-DATA-280421/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 8.15.1 allows remote anonymous attackers to enable and disable Jira Software configuration via a cross-site request forgery (CSRF) vulnerability. **CVE ID : CVE-2021-26071**		
Server-Side Request Forgery (SSRF)	01-04-2021	4	The WidgetConnector plugin in Confluence Server and Confluence Data Center before version 5.8.6 allowed remote attackers to manipulate the content of internal network resources via a blind Server-Side Request Forgery (SSRF) vulnerability. **CVE ID : CVE-2021-26072**	https://jira.atlassian.com/browse/CONFSERVER-61399	A-ATL-DATA-280421/43
N/A	15-04-2021	4	The Jira importers plugin AttachTemporaryFile rest resource in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before 8.13.4, and from version 8.14.0 before 8.15.1 allowed remote authenticated attackers to obtain the full path of the Jira application data directory via an information disclosure vulnerability in the error message when presented with an invalid filename. **CVE ID : CVE-2021-26075**	https://jira.atlassian.com/browse/JRASERVER-72316	A-ATL-DATA-280421/44
N/A	15-04-2021	4.3	The jira.editor.user.mode cookie set by the Jira Editor Plugin in Jira Server and Data Center before version 8.5.12, from version 8.6.0	https://jira.atlassian.com/browse/JRASERVER-	A-ATL-DATA-280421/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before version 8.13.4, and from version 8.14.0 before version 8.15.0 allows remote anonymous attackers who can perform an attacker in the middle attack to learn which mode a user is editing in due to the cookie not being set with a secure attribute if Jira was configured to use https. **CVE ID : CVE-2021-26076**	72252	
jira					
Cross-Site Request Forgery (CSRF)	01-04-2021	3.5	The SetFeatureEnabled.jspa resource in Jira Server and Data Center before version 8.5.13, from version 8.6.0 before version 8.13.5, and from version 8.14.0 before version 8.15.1 allows remote anonymous attackers to enable and disable Jira Software configuration via a cross-site request forgery (CSRF) vulnerability. **CVE ID : CVE-2021-26071**	https://jira.atlassian.com/browse/JRASERVER-72233	A-ATL-JIRA-280421/46
N/A	15-04-2021	4	The Jira importers plugin AttachTemporaryFile rest resource in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before 8.13.4, and from version 8.14.0 before 8.15.1 allowed remote authenticated attackers to obtain the full path of the Jira application data directory via an information disclosure	https://jira.atlassian.com/browse/JRASERVER-72316	A-ATL-JIRA-280421/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the error message when presented with an invalid filename. **CVE ID : CVE-2021-26075**		
N/A	15-04-2021	4.3	The jira.editor.user.mode cookie set by the Jira Editor Plugin in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before version 8.13.4, and from version 8.14.0 before version 8.15.0 allows remote anonymous attackers who can perform an attacker in the middle attack to learn which mode a user is editing in due to the cookie not being set with a secure attribute if Jira was configured to use https. **CVE ID : CVE-2021-26076**	https://jira.atlassian.com/browse/JRASERVER-72252	A-ATL-JIRA-280421/48
automattic					
wp_super_cache					
Improper Input Validation	05-04-2021	9	The WP Super Cache WordPress plugin before 1.7.2 was affected by an authenticated (admin+) RCE in the settings page due to input validation failure and weak $cache_path check in the WP Super Cache Settings -> Cache Location option. Direct access to the wp-cache-config.php file is not prohibited, so this vulnerability can be exploited for a web shell injection. **CVE ID : CVE-2021-24209**	https://plugins.trac.wordpress.org/changeset/2496238/wp-super-cache, https://wpscan.com/vulnerability/733d8a02-0d44-4b78-bbb2-37e447acd2f3	A-AUT-WP_S-280421/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
b2evolution					
b2evolution					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-04-2021	6.5	SQL Injection in the "evoadm.php" component of b2evolution v7.2.2-stable allows remote attackers to obtain sensitive database information by injecting SQL commands into the "cf_name" parameter when creating a new filter under the "Collections" tab. **CVE ID : CVE-2021-28242**	https://deadsh0t.medium.com/authenticated-boolean-based-blind-error-based-sql-injection-b752225f0644	A-B2E-B2EV-280421/50
backup-guard					
backup_guard					
Unrestricted Upload of File with Dangerous Type	05-04-2021	6.5	The WordPress Backup and Migrate Plugin â€“ Backup Guard WordPress plugin before 1.6.0 did not ensure that the imported files are of the SGBP format and extension, allowing high privilege users (admin+) to upload arbitrary files, including PHP ones, leading to RCE. **CVE ID : CVE-2021-24155**	https://wpscan.com/vulnerability/d442acac-4394-45e4-b6bb-adf4a40960fb	A-BAC-BACK-280421/51
btcpayserver					
btcpay_server					
N/A	01-04-2021	3.5	BTCPay Server before 1.0.7.1 mishandles the policy setting in which users can register (in Server Settings > Policies). This affects Docker use cases in which a mail server is configured. **CVE ID : CVE-2021-29251**	N/A	A-BTC-BTCP-280421/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
casap_automated_enrollment_system_project					
casap_automated_enrollment_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-04-2021	3.5	CASAP Automated Enrollment System version 1.0 contains a cross-site scripting (XSS) vulnerability through the Students > Edit > ROUTE parameter. **CVE ID : CVE-2021-27129**	N/A	A-CAS-CASA-280421/53
cern					
indico					
N/A	07-04-2021	5	CERN Indico before 2.3.4 can use an attacker-supplied Host header in a password reset link. **CVE ID : CVE-2021-30185**	N/A	A-CER-INDI-280421/54
chrono-node_project					
chrono-node					
N/A	12-04-2021	5	This affects the package chrono-node before 2.2.4. It hangs on a date-like string with lots of embedded spaces. **CVE ID : CVE-2021-23371**	https://github.com/wanasit/chrono/issues/382, https://github.com/wanasit/chrono/commit/98815b57622443b5c498a427210ebd603d705f4c, https://snyk.io/vuln/SNYK-JS-CHRONONODE-1083228	A-CHR-CHRO-280421/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cisco					
advanced_malware_protection_for_endpoints					
Uncontrolled Search Path Element	08-04-2021	7.2	A vulnerability in the dynamic link library (DLL) loading mechanism in Cisco Advanced Malware Protection (AMP) for Endpoints Windows Connector, ClamAV for Windows, and Immunet could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected Windows system. To exploit this vulnerability, the attacker would need valid credentials on the system. The vulnerability is due to insufficient validation of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on an affected system. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges. **CVE ID : CVE-2021-1386**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-tu79hvkO	A-CIS-ADVA-280421/56
clamav					
Uncontrolled Search Path Element	08-04-2021	7.2	A vulnerability in the dynamic link library (DLL) loading mechanism in Cisco Advanced Malware Protection (AMP) for Endpoints Windows Connector, ClamAV for Windows, and Immunet could allow an authenticated, local	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-	A-CIS-CLAM-280421/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform a DLL hijacking attack on an affected Windows system. To exploit this vulnerability, the attacker would need valid credentials on the system. The vulnerability is due to insufficient validation of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on an affected system. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges. **CVE ID : CVE-2021-1386**	tu79hvkO	
immunet					
Uncontrolled Search Path Element	08-04-2021	7.2	A vulnerability in the dynamic link library (DLL) loading mechanism in Cisco Advanced Malware Protection (AMP) for Endpoints Windows Connector, ClamAV for Windows, and Immunet could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected Windows system. To exploit this vulnerability, the attacker would need valid credentials on the system. The vulnerability is due to insufficient validation of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-tu79hvkO	A-CIS-IMMU-280421/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on an affected system. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges. **CVE ID : CVE-2021-1386**		
prime_license_manager					
Improper Control of Generation of Code ('Code Injection')	08-04-2021	9	A vulnerability in the SOAP API endpoint of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, and Cisco Prime License Manager could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by sending a SOAP API request with crafted parameters to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying Linux operating system of the affected device. **CVE ID : CVE-2021-1362**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-pqVYwyb	A-CIS-PRIM-280421/59
sd-wan_vmanage					
Improper Restriction of	08-04-2021	7.2	Multiple vulnerabilities in Cisco SD-WAN vManage	https://tools.cisco.c	A-CIS-SD-W-280421/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1137**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1479**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy	A-CIS-SD-W-280421/61
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.2	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy	A-CIS-SD-W-280421/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1480		
umbrella					
Improper Neutralization of Formula Elements in a CSV File	08-04-2021	6.8	Multiple vulnerabilities in the Admin audit log export feature and Scheduled Reports feature of Cisco Umbrella could allow an authenticated, remote attacker to perform formula and link injection attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1474**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-inject-gbZGHP5T	A-CIS-UMBR-280421/63
Improper Neutralization of Formula Elements in a CSV File	08-04-2021	3.5	Multiple vulnerabilities in the Admin audit log export feature and Scheduled Reports feature of Cisco Umbrella could allow an authenticated, remote attacker to perform formula and link injection attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1475**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-inject-gbZGHP5T	A-CIS-UMBR-280421/64
unified_communications_manager					
Improper Control of Generation of Code ('Code Injection')	08-04-2021	9	A vulnerability in the SOAP API endpoint of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-	A-CIS-UNIF-280421/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Unity Connection, and Cisco Prime License Manager could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by sending a SOAP API request with crafted parameters to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying Linux operating system of the affected device. **CVE ID : CVE-2021-1362**	pqVYwyb	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	A-CIS-UNIF-280421/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1380**		
Authentication Bypass by Assumed-Immutable Data	08-04-2021	4	A vulnerability in the Self Care Portal of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to modify data on an affected system without proper authorization. The vulnerability is due to insufficient validation of user-supplied data to the Self Care Portal. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to modify information without proper authorization. **CVE ID : CVE-2021-1399**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-selfcare-VRWWWHgE	A-CIS-UNIF-280421/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Externally-Accessible File or Directory	08-04-2021	4	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper inclusion of sensitive information in downloadable files. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to obtain hashed credentials of system users. To exploit this vulnerability an attacker would need to have valid user credentials with elevated privileges. **CVE ID : CVE-2021-1406**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-inf-disc-wCxZNjL2	A-CIS-UNIF-280421/68
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	A-CIS-UNIF-280421/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1407**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	A-CIS-UNIF-280421/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1408**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	A-CIS-UNIF-280421/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1409**		
unified_communications_manager_im_&_presence_service					
Improper Control of Generation of Code ('Code Injection')	08-04-2021	9	A vulnerability in the SOAP API endpoint of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, and Cisco Prime License Manager could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by sending a SOAP API request with crafted parameters to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying Linux operating system of the affected device. **CVE ID : CVE-2021-1362**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-pqVYwyb	A-CIS-UNIF-280421/72
Improper	08-04-2021	4.3	Multiple vulnerabilities in	https://to	A-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1380**	ols.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	280421/73
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-UNIF-280421/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1409**	cucm-xss-Q4PZcNzJ	
unified_contact_center_express					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-U2WTsUg6	A-CIS-UNIF-280421/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1463**		
unity_connection					
Improper Control of Generation of Code ('Code Injection')	08-04-2021	9	A vulnerability in the SOAP API endpoint of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, and Cisco Prime License Manager could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by sending a SOAP API request with crafted parameters to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying Linux operating	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-pqVYwyb	A-CIS-UNIT-280421/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system of the affected device. **CVE ID : CVE-2021-1362**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1380**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	A-CIS-UNIT-280421/77
Improper Neutralization of Input During Web	08-04-2021	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Unified	https://tools.cisco.com/security/center/	A-CIS-UNIT-280421/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2021-1409**	content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ	
webex_meetings					
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	08-04-2021	4.3	A vulnerability in certain web pages of Cisco Webex Meetings could allow an unauthenticated, remote attacker to modify a web page in the context of a user's browser. The vulnerability is due to improper checks on parameter values in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-VObwRK	A-CIS-WEBE-280421/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected pages. An attacker could exploit this vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. **CVE ID : CVE-2021-1420**	WV	
Improper Privilege Management	08-04-2021	4	A vulnerability in Cisco Webex Meetings for Android could allow an authenticated, remote attacker to modify the avatar of another user. This vulnerability is due to improper authorization checks. An attacker could exploit this vulnerability by sending a crafted request to the Cisco Webex Meetings client of a targeted user of a meeting in which they are both participants. A successful exploit could allow the attacker to modify the avatar of the targeted user. **CVE ID : CVE-2021-1467**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-andro-iac-f3UR8frB	A-CIS-WEBE-280421/80
citsmart					
citsmart					
Improper Neutralization of Special	06-04-2021	6.5	CITSmart before 9.1.2.28 mishandles the "filtro de autocomplete."	https://docs.citsmart.com/pt-	A-CIT-CITS-280421/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			**CVE ID : CVE-2021-28142**	br/citsmart-platform-9/get-started/about-citsmart/release-notes.html	
clamav					
clamav					
Improper Input Validation	08-04-2021	7.8	A vulnerability in the Excel XLM macro parsing module in Clam AntiVirus (ClamAV) Software versions 0.103.0 and 0.103.1 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper error handling that may result in an infinite loop. An attacker could exploit this vulnerability by sending a crafted Excel file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process hang, resulting in a denial of service condition. **CVE ID : CVE-2021-1252**	https://blog.clamav.net/2021/04/clamav-01032-security-patch-release.html	A-CLA-CLAM-280421/82
Improper Input Validation	08-04-2021	5	A vulnerability in the PDF parsing module in Clam AntiVirus (ClamAV) Software versions 0.103.0 and 0.103.1 could allow an unauthenticated, remote attacker to cause a denial of service condition on an	https://blog.clamav.net/2021/04/clamav-01032-security-patch-release.ht	A-CLA-CLAM-280421/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerability is due to improper buffer size tracking that may result in a heap buffer over-read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial of service condition. **CVE ID : CVE-2021-1404**	ml	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-04-2021	5	A vulnerability in the email parsing module in Clam AntiVirus (ClamAV) Software version 0.103.1 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper variable initialization that may result in an NULL pointer read. An attacker could exploit this vulnerability by sending a crafted email to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition. **CVE ID : CVE-2021-1405**	https://blog.clamav.net/2021/04/clamav-01032-security-patch-release.html	A-CLA-CLAM-280421/84
click-ranker					
click_ranker					
Improper Neutralizatio	07-04-2021	4.3	Cross-site scripting vulnerability in Click	N/A	A-CLI-CLIC-280421/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Ranker Ver.3.5 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20688**		
clogica					
seo_redirection					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The setting page of the SEO Redirection Plugin â€“ 301 Redirect Manager WordPress plugin through 6.3 is vulnerable to reflected Cross-Site Scripting (XSS) as user input is not properly sanitised before being output in an attribute. **CVE ID : CVE-2021-24187**	https://wpscan.com/vulnerability/c234700e-61dd-46a0-90fb-609e704269a9	A-CLO-SEO_-280421/86
cloudfoundry					
capi-release					
Insufficiently Protected Credentials	08-04-2021	4	Cloud Controller API versions prior to 1.106.0 logs service broker credentials if the default value of db logging config field is changed. CAPI database logs service broker password in plain text whenever a job to clean up orphaned items is run by Cloud Controller. **CVE ID : CVE-2021-22115**	https://www.cloudfoundry.org/blog/cve-2021-22115-capi-logs-service-broker-credentials/	A-CLO-CAPI-280421/87
cf-deployment					
Insufficiently Protected Credentials	08-04-2021	4	Cloud Controller API versions prior to 1.106.0 logs service broker credentials if the default value of db logging config field is changed. CAPI database logs service	https://www.cloudfoundry.org/blog/cve-2021-22115-capi-logs-	A-CLO-CF-D-280421/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			broker password in plain text whenever a job to clean up orphaned items is run by Cloud Controller. **CVE ID : CVE-2021-22115**	service-broker-credentials/	
cm-wp					
social_slider_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The Social Slider Widget WordPress plugin before 1.8.5 allowed Authenticated Reflected XSS in the plugin settings page as the â€˜token_errorâ€™ parameter can be controlled by users and it is directly echoed without being sanitized **CVE ID : CVE-2021-24196**	https://wpscan.com/vulnerability/bb20d732-a5e4-4140-ab51-b2aa1a53db12	A-CM--SOCI-280421/89
cohesity					
cohesity_dataplatform					
Use of Hard-coded Credentials	02-04-2021	7.5	Undocumented Default Cryptographic Key Vulnerability in Cohesity DataPlatform version 6.3 prior 6.3.1g, 6.4 up to 6.4.1c and 6.5.1 through 6.5.1b. The ssh key can provide an attacker access to the linux system in the affected version. **CVE ID : CVE-2021-28123**	https://github.com/cohesity/SecAdvisory/blob/master/CVE-2021-28123.md	A-COH-COHE-280421/90
Improper Authentication	02-04-2021	4.3	A man-in-the-middle vulnerability in Cohesity DataPlatform support channel in version 6.3 up to 6.3.1g, 6.4 up to 6.4.1c and 6.5.1 through 6.5.1b. Missing server authentication in impacted versions can allow an	https://github.com/cohesity/SecAdvisory/blob/master/CVE-2021-28124.md	A-COH-COHE-280421/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to Man-in-the-middle (MITM) support channel UI session to Cohesity DataPlatform cluster. **CVE ID : CVE-2021-28124**		
contribsys					
sidekiq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	4.3	Sidekiq through 5.1.3 and 6.x through 6.2.0 allows XSS via the queue name of the live-poll feature when Internet Explorer is used. **CVE ID : CVE-2021-30151**	https://github.com/mperham/sidekiq/issues/4852	A-CON-SIDE-280421/92
cozmoslabs					
user_profile_picture					
Exposure of Sensitive Information to an Unauthorized Actor	05-04-2021	5	The REST API endpoint get_users in the User Profile Picture WordPress plugin before 2.5.0 returned more information than was required for its functionality to users with the upload_files capability. This included password hashes, hashed user activation keys, usernames, emails, and other less sensitive information. **CVE ID : CVE-2021-24170**	https://wpscan.com/vulnerability/29fc5b0e-0a5f-4484-a1e6-a0a1206726cc	A-COZ-USER-280421/93
daifukuya					
kagemai					
Cross-Site Request Forgery (CSRF)	07-04-2021	6.8	Cross-site request forgery (CSRF) vulnerability in Kagemai 0.8.8 allows remote attackers to hijack the authentication of administrators via	N/A	A-DAI-KAGE-280421/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unspecified vectors. **CVE ID : CVE-2021-20687**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2021	4.3	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20686**	N/A	A-DAI-KAGE-280421/95
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2021	4.3	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20685**	N/A	A-DAI-KAGE-280421/96
database-backups_project					
database-backups					
Cross-Site Request Forgery (CSRF)	05-04-2021	5.8	The Database Backups WordPress plugin through 1.2.2.6 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as generate backups of the database, change the plugin's settings and delete backups. **CVE ID : CVE-2021-24174**	https://wpscan.com/vulnerability/350c3e9a-bcc2-486a-90e6-d1dc13ce1bd5	A-DAT-DATA-280421/97
dell					
system_update					
Uncontrolled Resource Consumption	02-04-2021	4.9	Dell System Update (DSU) 1.9 and earlier versions contain a denial of service vulnerability. A local authenticated malicious user with low privileges may potentially exploit this vulnerability to cause the	https://www.dell.com/support/kbdoc/en-us/000184608/dsa-2021-059-	A-DEL-SYST-280421/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system to run out of memory by running multiple instances of the vulnerable application. **CVE ID : CVE-2021-21529**	dell-emc-system-update-dsu-security-update-for-denial-of-service-vulnerability	
wyse_management_suite					
Improper Input Validation	02-04-2021	4	Wyse Management Suite versions up to 3.2 contains a vulnerability wherein a malicious authenticated user can cause a denial of service in the job status retrieval page, also affecting other users that would have normally access to the same subset of job details **CVE ID : CVE-2021-21533**	https://www.dell.com/support/kbdoc/en-us/000184666/dsa-2021-070-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-280421/99
deltaflow_project					
deltaflow					
Insufficiently Protected Credentials	06-04-2021	7.5	The Vangene deltaFlow E-platform does not take properly protective measures. Attackers can obtain privileged permissions remotely by tampering with users' data in the Cookie. **CVE ID : CVE-2021-28171**	N/A	A-DEL-DELT-280421/100
Improper Limitation of a Pathname	06-04-2021	5	There is a Path Traversal vulnerability in the file download function of	N/A	A-DEL-DELT-280421/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Vangene deltaFlow E-platform. Remote attackers can access credential data with this leakage. **CVE ID : CVE-2021-28172**		
Unrestricted Upload of File with Dangerous Type	06-04-2021	7.5	The file upload function of Vangene deltaFlow E-platform does not perform access controlled properly. Remote attackers can upload and execute arbitrary files without login. **CVE ID : CVE-2021-28173**	N/A	A-DEL-DELT-280421/102
devolutions					
devolutions_server					
N/A	01-04-2021	6.4	An issue was discovered in Devolutions Server before 2020.3. There is broken access control on Password List entry elements. **CVE ID : CVE-2021-23921**	https://devolutions.net/security/advisories/devo-2021-0002	A-DEV-DEVO-280421/103
Improper Authentication	01-04-2021	4.9	An issue was discovered in Devolutions Server before 2020.3. There is Broken Authentication with Windows domain users. **CVE ID : CVE-2021-23923**	https://devolutions.net/security/advisories/devo-2021-0002	A-DEV-DEVO-280421/104
Insertion of Sensitive Information into Log File	01-04-2021	5	An issue was discovered in Devolutions Server before 2020.3. There is an exposure of sensitive information in diagnostic files. **CVE ID : CVE-2021-23924**	https://devolutions.net/security/advisories/devo-2021-0002	A-DEV-DEVO-280421/105
Improper Neutralization of Input During Web	01-04-2021	4.3	An issue was discovered in Devolutions Server before 2020.3. There is a cross-site scripting (XSS)	https://devolutions.net/security/advisor	A-DEV-DEVO-280421/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			vulnerability in entries of type Document. **CVE ID : CVE-2021-23925**	ies/devo-2021-0002	
Origin Validation Error	14-04-2021	4.3	An overly permissive CORS policy in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-28048**	https://devolutions.net/security/advisories/DEVO-2021-0004	A-DEV-DEVO-280421/107
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-04-2021	6.5	An SQL Injection issue in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows an administrative user to execute arbitrary SQL commands via a username in api/security/userinfo/delete. **CVE ID : CVE-2021-28157**	https://devolutions.net/security/advisories/DEVO-2021-0004	A-DEV-DEVO-280421/108
remote_desktop_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2021	3.5	Cross-Site Scripting (XSS) in Administrative Reports in Devolutions Remote Desktop Manager before 2021.1 allows remote authenticated users to inject arbitrary web script or HTML via multiple input fields. **CVE ID : CVE-2021-28047**	https://devolutions.net/security/advisories/devo-2021-0003	A-DEV-REMO-280421/109
Improper Neutralization of Input During Web Page	01-04-2021	3.5	An issue was discovered in Devolutions Remote Desktop Manager before 2020.2.12. There is a cross-site scripting (XSS)	https://devolutions.net/security/advisories/devo-	A-DEV-REMO-280421/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability in webviews. **CVE ID : CVE-2021-23922**	2021-0001	
discord-recon_project					
discord-recon					
Improper Control of Generation of Code ('Code Injection')	09-04-2021	6.5	Discord Recon Server is a bot that allows you to do your reconnaissance process from your Discord. Remote code execution in version 0.0.1 would allow remote users to execute commands on the server resulting in serious issues. This flaw is patched in 0.0.2. **CVE ID : CVE-2021-21433**	https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-65fm-5x64-gv9x, https://github.com/DEMON1A/Discord-Recon/commit/26e2a084679679cccdeeabbb6889ce120eff7e50, https://github.com/DEMON1A/Discord-Recon/issues/6	A-DIS-DISC-280421/111
django-registration_project					
django-registration					
Generation of Error Message Containing Sensitive Information	01-04-2021	3.5	django-registration is a user registration package for Django. The django-registration package provides tools for implementing user-account registration flows in the Django web framework. In	https://github.com/ubernostrum/django-registration/security/advisorie	A-DJA-DJAN-280421/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			django-registration prior to 3.1.2, the base user-account registration view did not properly apply filters to sensitive data, with the result that sensitive data could be included in error reports rather than removed automatically by Django. Triggering this requires: A site is using django-registration < 3.1.2, The site has detailed error reports (such as Django's emailed error reports to site staff/developers) enabled and a server-side error (HTTP 5xx) occurs during an attempt by a user to register an account. Under these conditions, recipients of the detailed error report will see all submitted data from the account-registration attempt, which may include the user's proposed credentials (such as a password). **CVE ID : CVE-2021-21416**	s/GHSA-58c7-px5v-82hh	
djangoproject					
django					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	5	In Django 2.2 before 2.2.20, 3.0 before 3.0.14, and 3.1 before 3.1.8, MultiPartParser allowed directory traversal via uploaded files with suitably crafted file names. Built-in upload handlers were not affected by this vulnerability.	https://www.djangoproject.com/weblog/2021/apr/06/security-releases/, https://docs.djangoproject.com	A-DJA-DJAN-280421/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28658	/en/3.1/releases/security/	
dmasoftlab					
dma_radius_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	4.3	DMA Softlab Radius Manager 4.4.0 is affected by Cross Site Scripting (XSS) via the description, name, or address field (under admin.php). **CVE ID : CVE-2021-29011**	N/A	A-DMA-DMA_-280421/114
Reliance on Cookies without Validation and Integrity Checking	02-04-2021	7.5	DMA Softlab Radius Manager 4.4.0 assigns the same session cookie to every admin session. The cookie is valid when the admin is logged in, but is invalid (temporarily) during times when the admin is logged out. In other words, the cookie is functionally equivalent to a static password, and thus provides permanent access if stolen. **CVE ID : CVE-2021-29012**	N/A	A-DMA-DMA_-280421/115
radius_manager					
Cross-Site Request Forgery (CSRF)	07-04-2021	6.8	DMA Softlab Radius Manager 4.4.0 allows CSRF with impacts such as adding new manager accounts via admin.php. **CVE ID : CVE-2021-30147**	N/A	A-DMA-RADI-280421/116
docsifyjs					
docsify					
Improper Neutralization of Input	02-04-2021	4.3	docsify 4.12.1 is affected by Cross Site Scripting (XSS) because the search	N/A	A-DOC-DOCS-280421/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			component does not appropriately encode Code Blocks and mishandles the " character. **CVE ID : CVE-2021-30074**		
dolby					
audio_x2					
Untrusted Search Path	08-04-2021	4.6	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges. **CVE ID : CVE-2021-3146**	https://professional.dolby.com/siteassets/pdfs/dolby-dax2-security-advisory-2021-04-07.pdf	A-DOL-AUDI-280421/118
easy_contact_form_pro_project					
easy_contact_form_pro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The Easy Contact Form Pro WordPress plugin before 1.1.1.9 did not properly sanitise the text fields (such as Email Subject, Email Recipient, etc) when creating or editing a form, leading to an authenticated (author+) stored cross-site scripting issue. This could allow medium privilege accounts (such as author and editor) to perform XSS attacks against high privilege ones like administrator. **CVE ID : CVE-2021-24168**	https://wpscan.com/vulnerability/bfaa7d79-904e-45f1-bc42-ddd90a65ce74	A-EAS-EASY-280421/119
easy-form-builder-by-bitware_project					
easy-form-builder-by-bitware					
Unrestricted Upload of File	12-04-2021	6.5	The EFBP_verify_upload_file	https://wpscan.com	A-EAS-EASY-280421/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Dangerous Type			AJAX action of the Easy Form Builder WordPress plugin through 1.0, available to authenticated users, does not have any security in place to verify uploaded files, allowing low privilege users to upload arbitrary files, leading to RCE. **CVE ID : CVE-2021-24224**	/vulnerability/ed0c054b-54bf-4df8-9015-c76704c93484	
eaton					
intelligent_power_manager					
Improper Control of Generation of Code ('Code Injection')	13-04-2021	7.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated remote code execution vulnerability. IPM software does not sanitize the date provided via coverterCheckList action in meta_driver_srv.js class. Attackers can send a specially crafted packet to make IPM connect to rouge SNMP server and execute attacker-controlled code. **CVE ID : CVE-2021-23281**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/121
N/A	13-04-2021	7.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated eval injection vulnerability. The software does not neutralize code syntax from users before using in	https://www.eaton.com/content/dam/eaton/company/news-insights/c	A-EAT-INTE-280421/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the dynamic evaluation call in loadUserFile function under scripts/libs/utils.js. Successful exploitation can allow attackers to control the input to the function and execute attacker controlled commands. **CVE ID : CVE-2021-23277**	ybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated SQL injection. A malicious user can send a specially crafted packet to exploit the vulnerability. Successful exploitation of this vulnerability can allow attackers to add users in the data base. **CVE ID : CVE-2021-23276**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/123
Unrestricted Upload of File with Dangerous Type	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file upload vulnerability. IPM's maps_srv.js allows an attacker to upload a malicious NodeJS file using uploadBackgroud action.	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecuri	A-EAT-INTE-280421/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker can upload a malicious code or execute any command using a specially crafted packet to exploit the vulnerability. **CVE ID : CVE-2021-23280**	ty/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
Improper Input Validation	13-04-2021	6.4	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated arbitrary file delete vulnerability induced due to improper input validation in meta_driver_srv.js class with saveDriverData action using invalidated driverID. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23279**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/125
N/A	13-04-2021	5.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file delete vulnerability induced due to improper input validation at server/maps_srv.js with action removeBackground and	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/securit	A-EAT-INTE-280421/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server/node_upgrade_srv.js with action removeFirmware. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23278**	y-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
intelligent_power_manager_virtual_appliance					
N/A	13-04-2021	7.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated eval injection vulnerability. The software does not neutralize code syntax from users before using in the dynamic evaluation call in loadUserFile function under scripts/libs/utils.js. Successful exploitation can allow attackers to control the input to the function and execute attacker controlled commands. **CVE ID : CVE-2021-23277**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/127
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated SQL injection. A malicious user can send a specially crafted packet to exploit the vulnerability. Successful exploitation of this vulnerability can allow	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/securit	A-EAT-INTE-280421/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to add users in the data base. **CVE ID : CVE-2021-23276**	y-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
Unrestricted Upload of File with Dangerous Type	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file upload vulnerability. IPM's maps_srv.js allows an attacker to upload a malicious NodeJS file using uploadBackgroud action. An attacker can upload a malicious code or execute any command using a specially crafted packet to exploit the vulnerability. **CVE ID : CVE-2021-23280**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/129
Improper Input Validation	13-04-2021	6.4	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated arbitrary file delete vulnerability induced due to improper input validation in meta_driver_srv.js class with saveDriverData action using invalidated driverID. An attacker can send	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-	A-EAT-INTE-280421/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23279**	bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
N/A	13-04-2021	5.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file delete vulnerability induced due to improper input validation at server/maps_srv.js with action removeBackground and server/node_upgrade_srv.js with action removeFirmware. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23278**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/131
intelligent_power_protector					
N/A	13-04-2021	7.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated eval injection vulnerability. The software does not neutralize code syntax from users before using in the dynamic evaluation call in loadUserFile function under scripts/libs/utils.js.	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-	A-EAT-INTE-280421/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation can allow attackers to control the input to the function and execute attacker controlled commands. **CVE ID : CVE-2021-23277**	bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated SQL injection. A malicious user can send a specially crafted packet to exploit the vulnerability. Successful exploitation of this vulnerability can allow attackers to add users in the data base. **CVE ID : CVE-2021-23276**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/133
Unrestricted Upload of File with Dangerous Type	13-04-2021	6.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file upload vulnerability. IPM's maps_srv.js allows an attacker to upload a malicious NodeJS file using uploadBackgroud action. An attacker can upload a malicious code or execute any command using a	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/	A-EAT-INTE-280421/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted packet to exploit the vulnerability. **CVE ID : CVE-2021-23280**	eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	
Improper Input Validation	13-04-2021	6.4	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated arbitrary file delete vulnerability induced due to improper input validation in meta_driver_srv.js class with saveDriverData action using invalidated driverID. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23279**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf	A-EAT-INTE-280421/135
N/A	13-04-2021	5.5	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file delete vulnerability induced due to improper input validation at server/maps_srv.js with action removeBackground and server/node_upgrade_srv.js with action removeFirmware. An	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-	A-EAT-INTE-280421/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can send specially crafted packets to delete the files on the system where IPM software is installed. **CVE ID : CVE-2021-23278**	intelligent-power-manager-ipm-vulnerability-advisory.pdf	
eclipse					
jetty					
Improper Link Resolution Before File Access ('Link Following')	01-04-2021	4	In Eclipse Jetty 9.4.32 to 9.4.38, 10.0.0.beta2 to 10.0.1, and 11.0.0.beta2 to 11.0.1, if a user uses a webapps directory that is a symlink, the contents of the webapps directory is deployed as a static webapp, inadvertently serving the webapps themselves and anything else that might be in that directory. **CVE ID : CVE-2021-28163**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-j6qj-j888-vvgq	A-ECL-JETT-280421/137
Exposure of Sensitive Information to an Unauthorized Actor	01-04-2021	5	In Eclipse Jetty 9.4.37.v20210219 to 9.4.38.v20210224, the default compliance mode allows requests with URIs that contain %2e or %2e%2e segments to access protected resources within the WEB-INF directory. For example a request to /context/%2e/WEB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	https://github.com/eclipse/jetty.project/security/advisories/GHSA-v7ff-8wcx-gmc5	A-ECL-JETT-280421/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28164		
Uncontrolled Resource Consumption	01-04-2021	7.8	In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon receiving a large invalid TLS frame. **CVE ID : CVE-2021-28165**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-26vr-8j45-3r4w	A-ECL-JETT-280421/139
mosquitto					
NULL Pointer Dereference	07-04-2021	4	In Eclipse Mosquitto version 2.0.0 to 2.0.9, if an authenticated client that had connected with MQTT v5 sent a crafted CONNACK message to the broker, a NULL pointer dereference would occur. **CVE ID : CVE-2021-28166**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=572608	A-ECL-MOSQ-280421/140
eikisoft					
archive_collectively_operation_utility					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-04-2021	5.8	Directory traversal vulnerability in Archive collectively operation utility Ver.2.10.1.0 and earlier allows an attacker to create or overwrite files by leading a user to expand a malicious ZIP archives. **CVE ID : CVE-2021-20692**	http://www.eikisoft.com/release01.html	A-EIK-ARCH-280421/141
elbtide					
advanced_booking_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site	12-04-2021	3.5	The Advanced Booking Calendar WordPress plugin before 1.6.7 did not sanitise the calId GET parameter in the "Seasons & Calendars" page before outputing it in an A tag, leading to a	https://wpscan.com/vulnerability/25ca8af5-ab48-4e6d-b2ef-	A-ELB-ADVA-280421/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			reflected XSS issue **CVE ID : CVE-2021-24225**	fc291742f1d5, https://plugins.trac.wordpress.org/changeset/2503971/	
elementor					
website_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the column element (includes/elements/column.php) accepts an â€˜html_tagâ€™ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified â€˜save_builderâ€™ request containing JavaScript in the â€˜html_tagâ€™ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24201**	https://wpscan.com/vulnerability/9647f516-b130-4cc8-85fb-2e69b034ced0	A-ELE-WEBS-280421/143
Improper Neutralization of Input During Web Page Generation ('Cross-site	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the heading widget (includes/widgets/heading.php) accepts a 'header_size' parameter.	https://wpscan.com/vulnerability/b72bd13d-c8e2-4347-b009-	A-ELE-WEBS-280421/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request with this parameter set to 'script' and combined with a 'title' parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24202**	542fc0fe21bb	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the divider widget (includes/widgets/divider.php) accepts an 'html_tag' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request with this parameter set to 'script' and combined with a 'text' parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24203**	https://wpscan.com/vulnerability/aa152ad0-5b3d-4d1f-88f4-6899a546e72e	A-ELE-WEBS-280421/145
Improper Neutralization of Input During Web Page	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the accordion widget (includes/widgets/accordi	https://wpscan.com/vulnerability/772e172f-c8b4-	A-ELE-WEBS-280421/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			on.php) accepts a 'title_html_tag' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request containing JavaScript in the 'title_html_tag' parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24204**	4a6a-9eb9-9663295cfedf	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the icon box widget (includes/widgets/icon-box.php) accepts a 'title_size' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request containing JavaScript in the 'title_size' parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24205**	https://wpscan.com/vulnerability/ef23df6d-e265-44f6-bb94-1005b16d34d9	A-ELE-WEBS-280421/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	In the Elementor Website Builder WordPress plugin before 3.1.4, the image box widget (includes/widgets/image-box.php) accepts a 'title_size' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request containing JavaScript in the 'title_size' parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed. **CVE ID : CVE-2021-24206**	https://wpscan.com/vulnerability/2f66efd9-7d55-4f33-9109-3cb583a0c309	A-ELE-WEBS-280421/148
endian_trait_project					
endian_trait					
Double Free	01-04-2021	5	An issue was discovered in the endian_trait crate through 2021-01-04 for Rust. A double drop can occur when a user-provided Endian impl panics. **CVE ID : CVE-2021-29929**	https://rustsec.org/advisories/RUSTSEC-2021-0039.html	A-END-ENDI-280421/149
eng					
knowage					
Improper Neutralization of Special Elements used in an	05-04-2021	6.5	A SQL injection vulnerability in Knowage Suite version 7.1 exists in the documentexecution/url analytics driver component	N/A	A-ENG-KNOW-280421/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			via the 'par_year' parameter when running a report. **CVE ID : CVE-2021-30055**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-04-2021	3.5	A stored HTML injection vulnerability exists in Knowage Suite version 7.1. An attacker can inject arbitrary HTML in "/restful-services/2.0/analyticalDrivers" via the 'LABEL' and 'NAME' parameters. **CVE ID : CVE-2021-30057**	N/A	A-ENG-KNOW-280421/151
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	4.3	Knowage Suite before 7.4 is vulnerable to cross-site scripting (XSS). An attacker can inject arbitrary external script in '/knowagecockpitengine/api/1.0/pages/execute' via the 'SBI_HOST' parameter. **CVE ID : CVE-2021-30058**	N/A	A-ENG-KNOW-280421/152
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	Knowage Suite before 7.4 is vulnerable to reflected cross-site scripting (XSS). An attacker can inject arbitrary web script in /restful-services/publish via the 'EXEC_FROM' parameter that can lead to data leakage. **CVE ID : CVE-2021-30056**	N/A	A-ENG-KNOW-280421/153
entropymine					
deark					
Divide By Zero	14-04-2021	4.3	In Deark before v1.5.8, a specially crafted input file can cause a division by zero in (src/fmtutil.c) because of the value of pixelsize.	https://github.com/jsummers/deark/commit/62acb7753b0	A-ENT-DEAR-280421/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28856	e3c0d3ab3c15057b0a65222313334, https://fatihhcelik.github.io/posts/Division-By-Zero-Deark/	
NULL Pointer Dereference	14-04-2021	4.3	In Deark before 1.5.8, a specially crafted input file can cause a NULL pointer dereference in the dbuf_write function (src/deark-dbuf.c). **CVE ID : CVE-2021-28855**	https://github.com/jsummers/deark/commit/287f5ac31dfdc074669182f51ece637706070eeb, https://fatihhcelik.github.io/posts/NULL-Pointer-Dereference-Deark/	A-ENT-DEAR-280421/155
erlang					
erlang/otp					
Untrusted Search Path	09-04-2021	6.2	A local privilege escalation vulnerability was discovered in Erlang/OTP prior to version 23.2.3. By adding files to an existing installation's directory, a local attacker could hijack accounts of other users running Erlang programs or possibly coerce a service running with "erlsrv.exe" to execute arbitrary code as Local System. This can occur only under specific	N/A	A-ERL-ERLA-280421/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions on Windows with unsafe filesystem permissions. **CVE ID : CVE-2021-29221**		
esri					
arcgis_enterprise					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	3.5	A cross-site scripting (XSS) vulnerability in the Document Link of documents in ESRI ArcGIS Online before 10.9 and Enterprise before 10.9 allows remote authenticated users to inject arbitrary JavaScript code via a malicious HTML attribute such as onerror (in the URL field of the Parameters tab). **CVE ID : CVE-2021-3012**	N/A	A-ESR-ARCG-280421/157
arcgis_online					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	3.5	A cross-site scripting (XSS) vulnerability in the Document Link of documents in ESRI ArcGIS Online before 10.9 and Enterprise before 10.9 allows remote authenticated users to inject arbitrary JavaScript code via a malicious HTML attribute such as onerror (in the URL field of the Parameters tab). **CVE ID : CVE-2021-3012**	N/A	A-ESR-ARCG-280421/158
exiv2					
exiv2					
Improper Restriction of Operations	08-04-2021	6.4	A flaw was found in Exiv2 in versions before and including 0.27.4-RC1.	https://bugzilla.redhat.com/sh	A-EXI-EXIV-280421/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Improper input validation of the rawData.size property in Jp2Image::readMetadata() in jp2image.cpp can lead to a heap-based buffer overflow via a crafted JPG image containing malicious EXIF data. **CVE ID : CVE-2021-3482**	ow_bug.cgi?id=1946314	
expresstech					
quiz_and_survey_master					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-04-2021	6.5	The Quiz And Survey Master â€“ Best Quiz, Exam and Survey Plugin for WordPress plugin before 7.1.12 did not sanitise the result_id GET parameter on pages with the [qsm_result] shortcode without id attribute, concatenating it in a SQL statement and leading to an SQL injection. The lowest role allowed to use this shortcode in post or pages being author, such user could gain unauthorised access to the DBMS. If the shortcode (without the id attribute) is embed on a public page or post, then unauthenticated users could exploit the injection. **CVE ID : CVE-2021-24221**	https://plugins.trac.wordpress.org/changeset/2479603/, https://wpscan.com/vulnerability/3b52b25c-82a1-41c7-83ac-92e244f7c5ab	A-EXP-QUIZ-280421/160
responsive_menu					
Unrestricted Upload of File with Dangerous Type	05-04-2021	6.5	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, subscribers could upload zip archives containing malicious PHP files that	https://wpscan.com/vulnerability/066ba5d4-4aaa-4462-	A-EXP-RESP-280421/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would get extracted to the /rmp-menu/ directory. These files could then be accessed via the front end of the site to trigger remote code execution and ultimately allow an attacker to execute commands to further infect a WordPress site. **CVE ID : CVE-2021-24160**	b106-500c1f291c37	
Cross-Site Request Forgery (CSRF)	05-04-2021	6.8	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, attackers could craft a request and trick an administrator into uploading a zip archive containing malicious PHP files. The attacker could then access those files to achieve remote code execution and further infect the targeted site. **CVE ID : CVE-2021-24161**	https://wpscan.com/vulnerability/efca27e0-bdb6-4497-8330-081f909d6933	A-EXP-RESP-280421/162
Cross-Site Request Forgery (CSRF)	05-04-2021	6.8	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, attackers could craft a request and trick an administrator into importing all new settings. These settings could be modified to include malicious JavaScript, therefore allowing an attacker to inject payloads that could aid in further infection of the site. **CVE ID : CVE-2021-24162**	https://wpscan.com/vulnerability/923fc3a3-4bcc-4b48-870a-6150e14509b5	A-EXP-RESP-280421/163
ezxml_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ezxml					
NULL Pointer Dereference	11-04-2021	4.3	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_internal_dtd(), while parsing a crafted XML file, performs incorrect memory handling, leading to a NULL pointer dereference while running strcmp() on a NULL pointer. **CVE ID : CVE-2021-30485**	https://sourceforge.net/p/ezxml/bugs/25/	A-EZX-EZXM-280421/164
Out-of-bounds Write	15-04-2021	4.3	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_internal_dtd() performs incorrect memory handling while parsing crafted XML files, which leads to an out-of-bounds write of a one byte constant. **CVE ID : CVE-2021-31229**	https://sourceforge.net/p/ezxml/bugs/26/	A-EZX-EZXM-280421/165
facebook					
facebook					
Deserialization of Untrusted Data	12-04-2021	6.8	The run_action function of the Facebook for WordPress plugin before 3.0.0 deserializes user supplied data making it possible for PHP objects to be supplied creating an Object Injection vulnerability. There was also a useable magic method in the plugin that could be used to achieve remote code execution. **CVE ID : CVE-2021-24217**	https://wpscan.com/vulnerability/509f2754-a1a1-4142-9126-ae023a88533a	A-FAC-FACE-280421/166
Cross-Site	12-04-2021	6.8	The	https://w	A-FAC-FACE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			wp_ajax_save_fbe_settings and wp_ajax_delete_fbe_settings AJAX actions of the Facebook for WordPress plugin before 3.0.4 were vulnerable to CSRF due to a lack of nonce protection. The settings in the saveFbeSettings function had no sanitization allowing for script tags to be saved. **CVE ID : CVE-2021-24218**	pscan.com/vulnerability/169d21fc-d191-46ff-82e8-9ac887aed8a4	280421/167
thrift					
Release of Invalid Pointer or Reference	14-04-2021	7.5	An invalid free in Thrift's table-based serialization can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2021.02.22.00. **CVE ID : CVE-2021-24028**	https://github.com/facebook/fbthrift/commit/bfda1efa547dce11a38592820916db01b05b9339, https://www.facebook.com/security/advisories/cve-2021-24028	A-FAC-THRI-280421/168
ffmpeg					
ffmpeg					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-04-2021	6.8	FFmpeg <=4.3 contains a buffer overflow vulnerability in libavcodec through a crafted file that may lead to remote code execution. **CVE ID : CVE-2021-30123**	http://git.videolan.org/?p=ffmpeg.git;a=commitdiff;h=d6f293353c94c7ce200f6e09	A-FFM-FFMP-280421/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				75ae3de49787f91f, https://trac.ffmpeg.org/ticket/8863, https://trac.ffmpeg.org/ticket/8845	
fireeye					
email_malware_protection_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-04-2021	4	eMPS 9.0.1.923211 on FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the sort_by parameter to the email search feature. According to the vendor, the issue is fixed in 9.0.3. NOTE: this is different from CVE-2020-25034 and affects newer versions of the software. **CVE ID : CVE-2021-28969**	N/A	A-FIR-EMAI-280421/170
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-04-2021	4	eMPS 9.0.1.923211 on the Central Management of FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the job_id parameter to the email search feature. According to the vendor, the issue is fixed in 9.0.3. **CVE ID : CVE-2021-28970**	N/A	A-FIR-EMAI-280421/171
fluidsynth					
fluidsynth					
Use After	13-04-2021	7.5	FluidSynth 2.1.7 contains a	N/A	A-FLU-FLUI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			use after free vulnerability in sfloader/fluid_sffile.c that can result in arbitrary code execution or a denial of service (DoS) if a malicious soundfont2 file is loaded into a fluidsynth library. **CVE ID : CVE-2021-28421**		280421/172
forescout					
counteract					
Incorrect Default Permissions	14-04-2021	4.4	An issue was discovered in Forescout CounterACT before 8.1.4. A local privilege escalation vulnerability is present in the logging function. SecureConnector runs with administrative privileges and writes logs entries to a file in %PROGRAMDATA%\ForeScout SecureConnector\ that has full permissions for the Everyone group. Using a symbolic link allows an attacker to point the log file to a privileged location such as %WINDIR%\System32. The resulting log file adopts the file permissions of the source of the symbolic link (in this case, the Everyone group). The log file in System32 can be replaced and renamed with a malicious DLL for DLL hijacking. **CVE ID : CVE-2021-28098**	https://docs.forescout.com	A-FOR-COUN-280421/173
fortinet					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fortiadc					
Insertion of Sensitive Information into Log File	12-04-2021	4	A clear text storage of sensitive information into log file vulnerability in FortiADCManager 5.3.0 and below, 5.2.1 and below and FortiADC 5.3.7 and below may allow a remote authenticated attacker to read other local users' password in log files. **CVE ID : CVE-2021-24024**	https://fortiguard.com/advisory/FG-IR-19-244	A-FOR-FORT-280421/174
fortiadc_manager					
Insertion of Sensitive Information into Log File	12-04-2021	4	A clear text storage of sensitive information into log file vulnerability in FortiADCManager 5.3.0 and below, 5.2.1 and below and FortiADC 5.3.7 and below may allow a remote authenticated attacker to read other local users' password in log files. **CVE ID : CVE-2021-24024**	https://fortiguard.com/advisory/FG-IR-19-244	A-FOR-FORT-280421/175
friendica					
friendica					
Missing Release of Memory after Effective Lifetime	05-04-2021	5	** DISPUTED ** Module/Settings/UserExport.php in Friendica through 2021.01 allows settings/userexport to be used by anonymous users, as demonstrated by an attempted access to an array offset on a value of type null, and excessive memory consumption. NOTE: the vendor states "the feature still requires a valid authentication cookie even if the route is	https://github.com/friendica/friendica/pull/10113/commits/acbcc56754121ba080eac5b6fdf69e64ed7fe453	A-FRI-FRIE-280421/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible to non-logged users." **CVE ID : CVE-2021-30141**		
froala					
froala_editor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	4.3	Froala Editor 3.2.6 is affected by Cross Site Scripting (XSS). Under certain conditions, a base64 crafted string leads to persistent Cross-site scripting (XSS) vulnerability within the hyperlink creation module. **CVE ID : CVE-2021-30109**	N/A	A-FRO-FROA-280421/177
getgrav					
grav					
Improper Control of Generation of Code ('Code Injection')	13-04-2021	6.5	Grav is a file based Web-platform. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. The issue was addressed in version 1.7.11. **CVE ID : CVE-2021-29440**	https://github.com/getgrav/grav/security/advisories/GHSA-g8r4-p96j-xfxc	A-GET-GRAV-280421/178
grav_admin					
Incorrect Authorization	13-04-2021	6.5	The Grav admin plugin prior to version 1.10.11 does not correctly verify caller's privileges. As a consequence, users with the permission	https://github.com/getgrav/grav-plugin-admin/security/advi	A-GET-GRAV-280421/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`admin.login` can install third-party plugins and their dependencies. By installing the right plugin, an attacker can obtain an arbitrary code execution primitive and elevate their privileges on the instance. The vulnerability has been addressed in version 1.10.11. As a mitigation blocking access to the `/admin` path from untrusted sources will reduce the probability of exploitation. **CVE ID : CVE-2021-29439**	sories/GHSA-wg37-cf5x-55hq	
grav-plugin-admin					
Improper Access Control	07-04-2021	7.5	Grav Admin Plugin is an HTML user interface that provides a way to configure Grav and create and modify pages. In versions 1.10.7 and earlier, an unauthenticated user can execute some methods of administrator controller without needing any credentials. Particular method execution will result in arbitrary YAML file creation or content change of existing YAML files on the system. Successfully exploitation of that vulnerability results in configuration changes, such as general site information change, custom scheduler job definition, etc. Due to the nature of the vulnerability, an adversary can change some part of	https://github.com/getgrav/grav-plugin-admin/security/advisories/GHSA-6f53-6qgv-39pj	A-GET-GRAV-280421/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the webpage, or hijack an administrator account, or execute operating system command under the context of the web-server user. This vulnerability is fixed in version 1.10.8. Blocking access to the `/admin` path from untrusted sources can be applied as a workaround. **CVE ID : CVE-2021-21425**		
github					
enterprise_server					
Incorrect Authorization	02-04-2021	4.3	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed access tokens generated from a GitHub App's web authentication flow to read private repository metadata via the REST API without having been granted the appropriate permissions. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. The private repository metadata returned would be limited to repositories owned by the user the token identifies. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.4 and was fixed in versions 3.0.4, 2.22.10, 2.21.18. This vulnerability	https://docs.github.com/en/enterprise-server@2.21/admin/release-notes#2.21.18, https://docs.github.com/en/enterprise-server@2.22/admin/release-notes#2.22.10, https://docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.4	A-GIT-ENTE-280421/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2021-22865**		
gitlab					
gitlab					
Uncontrolled Resource Consumption	01-04-2021	4	Potential DoS was identified in gitlab-shell in GitLab CE/EE version 12.6.0 or above, which allows an attacker to spike the server resource utilization via gitlab-shell command. **CVE ID : CVE-2021-22177**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22177.json	A-GIT-GITL-280421/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	3.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4. It was possible to exploit a stored cross-site-scripting in merge request via a specifically crafted branch name. **CVE ID : CVE-2021-22196**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22196.json	A-GIT-GITL-280421/183
Loop with Unreachable Exit Condition ('Infinite Loop')	02-04-2021	4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.6 where an infinite loop exist when an authenticated user with specific rights access a MR having source and target branch pointing to each other **CVE ID : CVE-2021-22197**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22197.json	A-GIT-GITL-280421/184
N/A	02-04-2021	4	An issue has been discovered in GitLab CE/EE affecting all versions from 13.8 and above allowing an authenticated user to	https://gitlab.com/gitlab-org/cves/-/blob/mas	A-GIT-GITL-280421/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delete incident metric images of public projects. **CVE ID : CVE-2021-22198**	ter/2021/CVE-2021-22198.json	
N/A	02-04-2021	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.6. Under a special condition it was possible to access data of an internal repository through a public project fork as an anonymous user. **CVE ID : CVE-2021-22200**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22200.json	A-GIT-GITL-280421/186
N/A	02-04-2021	4	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.9. A specially crafted import file could read files on the server. **CVE ID : CVE-2021-22201**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22201.json	A-GIT-GITL-280421/187
Cross-Site Request Forgery (CSRF)	02-04-2021	4.3	An issue has been discovered in GitLab CE/EE affecting all previous versions. If the victim is an admin, it was possible to issue a CSRF in System hooks through the API. **CVE ID : CVE-2021-22202**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22202.json	A-GIT-GITL-280421/188
N/A	02-04-2021	5	An issue has been discovered in GitLab CE/EE affecting all versions starting with 13.7.9. A specially crafted Wiki page allowed attackers to read arbitrary files on the server. **CVE ID : CVE-2021-22203**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22203.json	A-GIT-GITL-280421/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-04-2021	4	A path traversal vulnerability via the GitLab Workhorse in all versions of GitLab could result in the leakage of a JWT token **CVE ID : CVE-2021-22190**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22190.json	A-GIT-GITL-280421/190
gitlab-vscode-extension					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-04-2021	6.8	Client side code execution in gitlab-vscode-extension v3.15.0 and earlier allows attacker to execute code on user system **CVE ID : CVE-2021-22195**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22195.json	A-GIT-GITL-280421/191
givewp					
give					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	The GiveWP â€“ Donation Plugin and Fundraising Platform WordPress plugin before 2.10.0 was affected by a reflected Cross-Site Scripting vulnerability inside of the administration panel, via the 's' GET parameter on the Donors page. **CVE ID : CVE-2021-24213**	https://wpscan.com/vulnerability/da4ab508-a423-4c7f-a1d4-42ec6f989309	A-GIV-GIVE-280421/192
glpi-project					
dashboard					
Incorrect Authorization	06-04-2021	4	The Dashboard plugin through 1.0.2 for GLPI allows remote low-privileged users to bypass access control on viewing information about the last ten events, the connected	https://plugins.glpi-project.org/#/plugin/dashboard	A-GLP-DASH-280421/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users, and the users in the tech category. For example, plugins/dashboard/front/main2.php can be used. **CVE ID : CVE-2021-30144**		
gnu					
binutils					
Improper Input Validation	15-04-2021	7.1	There's a flaw in the BFD library of binutils in versions before 2.36. An attacker who supplies a crafted file to an application linked with BFD, and using the DWARF functionality, could cause an impact to system availability by way of excessive memory consumption. **CVE ID : CVE-2021-3487**	https://bugzilla.redhat.com/show_bug.cgi?id=1947111	A-GNU-BINU-280421/194
chess					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-04-2021	6.8	GNU Chess 6.2.7 allows attackers to execute arbitrary code via crafted PGN (Portable Game Notation) data. This is related to a buffer overflow in the use of a .tmp.epd temporary file in the cmd_pgnload and cmd_pgnreplay functions in frontend/cmd.cc. **CVE ID : CVE-2021-30184**	https://lists.gnu.org/archive/html/bug-gnu-chess/2021-04/msg00000.html, https://lists.gnu.org/archive/html/bug-gnu-chess/2021-04/msg00001.html	A-GNU-CHES-280421/195
go-vela					
vela					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	09-04-2021	3.5	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. An authentication mechanism added in version 0.7.0 enables some malicious user to obtain secrets utilizing the injected credentials within the `~/.netrc` file. Refer to the referenced GitHub Security Advisory for complete details. This is fixed in version 0.7.5. **CVE ID : CVE-2021-21432**	https://github.com/go-vela/server/commit/cb4352918b8ecace9fe969b90404d337b0744d46, https://github.com/go-vela/server/pull/337, https://github.com/go-vela/server/security/advisories/GHSA-8j3f-mhq8-gmh4	A-GO--VELA-280421/196
google					
chrome					
Out-of-bounds Write	09-04-2021	6.8	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21197**	https://crbug.com/1173903, https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-280421/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-04-2021	6.8	Heap buffer overflow in TabStrip in Google Chrome on Windows prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21196**	https://crbug.com/1175992, https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-280421/198
Use After Free	09-04-2021	6.8	Use after free in V8 in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21195**	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html, https://crbug.com/1182647	A-GOO-CHRO-280421/199
Use After Free	09-04-2021	6.8	Use after free in screen sharing in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21194**	https://crbug.com/1181228, https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-280421/200
Use After	09-04-2021	6.8	Use after free in Aura in	https://cr	A-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			Google Chrome on Linux prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21199**	bug.com/1179635, https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html	CHRO-280421/201
Out-of-bounds Read	09-04-2021	4.3	Out of bounds read in IPC in Google Chrome prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-21198**	https://crbug.com/1184399, https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-280421/202
gpac					
gpac					
NULL Pointer Dereference	14-04-2021	7.5	NULL Pointer Dereference in the "isomedia/track.c" module's "MergeTrack()" function of GPAC v0.5.2 allows attackers to execute arbitrary code or cause a Denial-of-Service (DoS) by uploading a malicious MP4 file. **CVE ID : CVE-2021-28300**	N/A	A-GPA-GPAC-280421/203
gradle					
gradle					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insecure Temporary File	12-04-2021	1.9	In Gradle before version 7.0, files created with open permissions in the system temporary directory can allow an attacker to access information downloaded by Gradle. Some builds could be vulnerable to a local information disclosure. Remote files accessed through TextResourceFactory are downloaded into the system temporary directory first. Sensitive information contained in these files can be exposed to other local users on the same system. If you do not use the `TextResourceFactory` API, you are not vulnerable. As of Gradle 7.0, uses of the system temporary directory have been moved to the Gradle User Home directory. By default, this directory is restricted to the user running the build. As a workaround, set a more restrictive umask that removes read access to other users. When files are created in the system temporary directory, they will not be accessible to other users. If you are unable to change your system's umask, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit	https://github.com/gradle/gradle/security/advisories/GHSA-fp8h-qmr5-j4c8, https://docs.gradle.org/7.0/release-notes.html#security-advisories	A-GRA-GRAD-280421/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions to the build user only. **CVE ID : CVE-2021-29429**		
group-office					
group_office					
Server-Side Request Forgery (SSRF)	14-04-2021	5	A Server-Side Request Forgery (SSRF) vulnerability in Group Office 6.4.196 allows a remote attacker to forge GET requests to arbitrary URLs via the url parameter to group/api/upload.php. **CVE ID : CVE-2021-28060**	N/A	A-GRO-GROU-280421/205
handlebarsjs					
handlebars					
N/A	12-04-2021	7.5	The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source. **CVE ID : CVE-2021-23369**	https://github.com/handlebars-lang/handlebars.js/commit/b6d3de7123eebba603e321f04afdbae608e8fea8, https://github.com/handlebars-lang/handlebars.js/commit/f05897016982685781 99be25285b2ebea1c1e427	A-HAN-HAND-280421/206
haxx					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libcurl					
Exposure of Sensitive Information to an Unauthorized Actor	01-04-2021	5	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request. **CVE ID : CVE-2021-22876**	https://curl.se/docs/CVE-2021-22876.html	A-HAX-LIBC-280421/207
Authentication Bypass by Spoofing	01-04-2021	4.3	curl 7.63.0 to and including 7.75.0 includes vulnerability that allows a malicious HTTPS proxy to MITM a connection due to bad handling of TLS 1.3 session tickets. When using a HTTPS proxy and TLS 1.3, libcurl can confuse session tickets arriving from the HTTPS proxy but work as if they arrived from the remote server and then wrongly "short-cut" the host handshake. When confusing the tickets, a HTTPS proxy can trick libcurl to use the wrong session ticket resume for the host and thereby circumvent the server TLS certificate check and make a MITM attack to be possible to perform	https://curl.se/docs/CVE-2021-22890.html	A-HAX-LIBC-280421/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unnoticed. Note that such a malicious HTTPS proxy needs to provide a certificate that curl will accept for the MITMed server for an attack to work - unless curl has been told to ignore the server certificate check. **CVE ID : CVE-2021-22890**		
hpe					
integrated_lights-out_amplifier					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2021	4.3	A potential security vulnerability has been identified in HPE iLO Amplifier Pack. The vulnerability could be remotely exploited to allow Cross-Site Scripting (XSS). HPE has provided the following software update to resolve the vulnerability in HPE iLO Amplifier Pack: HPE iLO Amplifier Pack 1.80 or later. **CVE ID : CVE-2021-26580**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04107en_us	A-HPE-INTE-280421/209
htmldoc_project					
htmldoc					
Integer Overflow or Wraparound	05-04-2021	7.5	Integer overflow in the htmldoc 1.9.11 and before may allow attackers to execute arbitrary code and cause a denial of service that is similar to CVE-2017-9181. **CVE ID : CVE-2021-20308**	N/A	A-HTM-HTML-280421/210
htmly					
htmly					
Improper Neutralizatio	13-04-2021	3.5	htmly 2.8.0 allows stored XSS via the blog title,	N/A	A-HTM-HTML-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Tagline, or Description to config.html.php. **CVE ID : CVE-2021-30637**		280421/211
ibm					
collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-COLL-280421/212
doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-DOOR-280421/213
engineering_insights					
Improper Neutralization of Input During Web Page	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-ENGI-280421/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	es/198441, https://www.ibm.com/support/pages/node/6441803	
engineering_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-ENGI-280421/215
engineering_requirements_management_doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-ENGI-280421/216
engineering_test_management					
Improper Neutralization of Input During Web	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users	https://exchange.xforce.ibmcloud.com/vu	A-IBM-ENGI-280421/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	lnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-ENGI-280421/218
rational_engineering_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-RATI-280421/219
rational_quality_manager					
Improper Neutralization of Input	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This	https://exchange.xforce.ibmclo	A-IBM-RATI-280421/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	ud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	
rational_team_concert					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-RATI-280421/221
removable_media_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	A-IBM-REMO-280421/222
rhapsody_model_manager					
Improper Neutralizatio	12-04-2021	4.3	IBM Jazz Team Server products are vulnerable to	https://exchange.xfo	A-IBM-RHAP-280421/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198441. **CVE ID : CVE-2021-20519**	rce.ibmcloud.com/vulnerabilities/198441, https://www.ibm.com/support/pages/node/6441803	
spectrum_scale					
Incorrect Authorization	09-04-2021	1.9	IBM Spectrum Scale 5.1.0.1 could allow a local attacker to bypass the filesystem audit logging mechanism when file audit logging is enabled. IBM X-Force ID: 199478. **CVE ID : CVE-2021-29671**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199478, https://www.ibm.com/support/pages/node/6441429	A-IBM-SPEC-280421/224
websphere_application_server					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	A-IBM-WEBS-280421/225
id-map_project					
id-map					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-04-2021	7.5	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in remove_set upon a panic in a Drop impl. **CVE ID : CVE-2021-30457**	N/A	A-ID--ID-M-280421/226
Double Free	07-04-2021	7.5	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in get_or_insert upon a panic of a user-provided f function. **CVE ID : CVE-2021-30456**	N/A	A-ID--ID-M-280421/227
Double Free	07-04-2021	7.5	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in IdMap::clone_from upon a .clone panic. **CVE ID : CVE-2021-30455**	N/A	A-ID--ID-M-280421/228
insert_many_project					
insert_many					
Double Free	01-04-2021	5	An issue was discovered in the insert_many crate through 2021-01-26 for Rust. Elements may be dropped twice if a .next() method panics. **CVE ID : CVE-2021-29933**	https://rustsec.org/advisories/RUSTSEC-2021-0042.html	A-INS-INSE-280421/229
jamf					
jamf					
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-04-2021	4.3	Jamf Pro before 10.28.0 allows XSS related to inventory history, aka PI-009376. **CVE ID : CVE-2021-30125**	https://docs.jamf.com/10.28.0/jamf-pro/release-notes/Bug	A-JAM-JAMF-280421/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				_Fixes_and_Enhancements.html	
jazzband					
django_debug_toolbar					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-04-2021	7.5	A SQL Injection issue in the SQL Panel in Jazzband Django Debug Toolbar before 1.11.1, 2.x before 2.2.1, and 3.x before 3.2.1 allows attackers to execute SQL statements by changing the raw_sql input field of the SQL explain, analyze, or select form. **CVE ID : CVE-2021-30459**	https://github.com/jazzband/django-debug-toolbar/security/advisories/GHSA-pghf-347x-c2gj, https://www.djangoproject.com/weblog/2021/apr/14/debug-toolbar-security-releases/	A-JAZ-DJAN-280421/231
jenkins					
jenkins					
Improper Input Validation	07-04-2021	4	Jenkins 2.286 and earlier, LTS 2.277.1 and earlier does not validate the type of object created after loading the data submitted to the `config.xml` REST API endpoint of a node, allowing attackers with Computer/Configure permission to replace a node with one of a different type. **CVE ID : CVE-2021-21639**	https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-1721	A-JEN-JENK-280421/232
Improper	07-04-2021	4	Jenkins 2.286 and earlier,	https://w	A-JEN-JENK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Handling of Inconsistent Structural Elements			LTS 2.277.1 and earlier does not properly check that a newly created view has an allowed name, allowing attackers with View/Create permission to create views with invalid or already-used names. **CVE ID : CVE-2021-21640**	ww.jenkins.io/security/advisory/2021-04-07/#SECURITY-1871	280421/233
promoted_builds					
Cross-Site Request Forgery (CSRF)	07-04-2021	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins promoted builds Plugin 3.9 and earlier allows attackers to to promote builds. **CVE ID : CVE-2021-21641**	https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-2293	A-JEN-PROM-280421/234
jh_404_logger_project					
jh_404_logger					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The JH 404 Logger WordPress plugin through 1.1 doesn't sanitise the referer and path of 404 pages, when they are output in the dashboard, which leads to executing arbitrary JavaScript code in the WordPress dashboard. **CVE ID : CVE-2021-24176**	https://wpscan.com/vulnerability/705bcd6e-6817-4f89-be37-901a767b0585	A-JH_-JH_4-280421/235
jitsi					
meet					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2021	4.3	Cross Site Scripting (XSS) in the Jitsi Meet 2.7 through 2.8.3 plugin for Moodle via the "sessionpriv.php" module. This allows attackers to craft a malicious URL, which when clicked on by users, can inject javascript code to be	N/A	A-JIT-MEET-280421/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			run by the application. **CVE ID : CVE-2021-26812**		
joomla					
joomla!					
N/A	14-04-2021	5	An issue was discovered in Joomla! 3.0.0 through 3.9.25. Inadequate filters on module layout settings could lead to an LFI. **CVE ID : CVE-2021-26031**	https://developer.joomla.org/security-centre/851-20210402-core-inadequate-filters-on-module-layout-settings.html	A-JOO-JOOM-280421/237
jsrsasign_project					
jsrsasign					
Improper Verification of Cryptographic Signature	07-04-2021	6.4	In the jsrsasign package through 10.1.13 for Node.js, some invalid RSA PKCS#1 v1.5 signatures are mistakenly recognized to be valid. NOTE: there is no known practical attack. **CVE ID : CVE-2021-30246**	N/A	A-JSR-JSRS-280421/238
kaspersky					
internet_security					
Incorrect Authorization	01-04-2021	2.1	KIS for macOS in some use cases was vulnerable to AV bypass that potentially allowed an attacker to disable anti-virus protection. **CVE ID : CVE-2021-26718**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#310321	A-KAS-INTE-280421/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
kiboit					
phastpress					
URL Redirection to Untrusted Site ('Open Redirect')	05-04-2021	5.8	There is an open redirect in the PhastPress WordPress plugin before 1.111 that allows an attacker to malform a request to a page with the plugin and then redirect the victim to a malicious page. There is also a support comment from another user one year ago (https://wordpress.org/support/topic/phast-php-used-for-remote-fetch/) that says that the php involved in the request only go to whitelisted pages but it's possible to redirect the victim to any domain. **CVE ID : CVE-2021-24210**	https://plugins.trac.wordpress.org/changeset/2497610/, https://wpscan.com/vulnerability/9b3c5412-8699-49e8-b60c-20d2085857fb	A-KIB-PHAS-280421/240
latrix_project					
latrix					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2021	7.5	An issue was discovered in LATRIX 0.6.0. SQL injection in the txtaccesscode parameter of inandout.php leads to information disclosure and code execution. **CVE ID : CVE-2021-30000**	N/A	A-LAT-LATR-280421/241
learnsite_project					
learnsite					
Improper Privilege Management	08-04-2021	6.5	Learnsite 1.2.5.0 contains a remote privilege escalation vulnerability in /Manager/index.aspx through the JudgIsAdmin()	N/A	A-LEA-LEAR-280421/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function. By modifying the initial letter of the key of a user cookie, the key of the administrator cookie can be obtained. **CVE ID : CVE-2021-27522**		
libexif_project					
exif					
NULL Pointer Dereference	14-04-2021	4.3	NULL Pointer Deference in the exif command line tool, when printing out XML formatted EXIF data, in exif v0.6.22 and earlier allows attackers to cause a Denial of Service (DoS) by uploading a malicious JPEG file, causing the application to crash. **CVE ID : CVE-2021-27815**	https://github.com/libexif/exif/commit/eb84b0e3c5f2a86013b6fcfb800d187896a648fa, https://github.com/libexif/exif/commit/f6334d9d32437ef13dc902f0a88a2be0063d9d1c	A-LIB-EXIF-280421/243
libpano13_project					
libpano13					
Use of Externally-Controlled Format String	05-04-2021	7.5	Format string vulnerability in panoFileOutputNamesCreate() in libpano13 2.9.20~rc2+dfsg-3 and earlier can lead to read and write arbitrary memory values. **CVE ID : CVE-2021-20307**	N/A	A-LIB-LIBP-280421/244
libretro					
retroarch					
Improper	07-04-2021	4.6	The text-to-speech engine	http://libr	A-LIB-RETR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			in libretro RetroArch for Windows 0.11 passes unsanitized input to PowerShell through platform_win32.c via the accessibility_speak_windows function, which allows attackers who have write access on filesystems that are used by RetroArch to execute code via command injection using specially a crafted file and directory names. **CVE ID : CVE-2021-28927**	etro.com, https://github.com/libretro/RetroArch/blob/d3dc3ee989ec6a4903c689907ffc47027f71f776/frontend/drivers/platform_win32.c	280421/245
lightcms_project					
lightcms					
N/A	15-04-2021	7.5	LightCMS v1.3.5 contains a remote code execution vulnerability in /app/Http/Controllers/Admin/NEditorController.php during the downloading of external images. **CVE ID : CVE-2021-27112**	N/A	A-LIG-LIGH-280421/246
lightmeter					
controlcenter					
N/A	02-04-2021	6.4	Lightmeter ControlCenter 1.1.0 through 1.5.x before 1.5.1 allows anyone who knows the URL of a publicly available Lightmeter instance to access application settings, possibly including an SMTP password and a Slack access token, via a settings HTTP query. **CVE ID : CVE-2021-30126**	https://lightmeter.io/lightmeter-1-5-1-important-security-fixes/	A-LIG-CONT-280421/247
likebtn-like-button_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
likebtn-like-button					
Server-Side Request Forgery (SSRF)	05-04-2021	5	The LikeBtn WordPress Like Button Rating â™¥ LikeBtn WordPress plugin before 2.6.32 was vulnerable to Unauthenticated Full-Read Server-Side Request Forgery (SSRF). **CVE ID : CVE-2021-24150**	https://wpscan.com/vulnerability/6bc6023f-a5e7-4665-896c-95afa5b638fb	A-LIK-LIKE-280421/248
linuxfoundation					
umoci					
Improper Input Validation	06-04-2021	2.1	Open Container Initiative umoci before 0.4.7 allows attackers to overwrite arbitrary host paths via a crafted image that causes symlink traversal when "umoci unpack" or "umoci raw unpack" is used. **CVE ID : CVE-2021-29136**	https://github.com/opencontainers/umoci/security/advisories/GHSA-9m95-8hx6-7p9v, http://www.openwall.com/lists/oss-security/2021/04/06/2, https://github.com/opencontainers/umoci/commit/d9efc31daf2206f7d3fdb839863cf7a576a2eb57	A-LIN-UMOC-280421/249
liquidfiles					
liquidfiles					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	3.5	LiquidFiles 3.4.15 has stored XSS through the "send email" functionality when sending a file via email to an administrator. When a file has no extension and contains malicious HTML / JavaScript content (such as SVG with HTML content), the payload is executed upon a click. This is fixed in 3.5. **CVE ID : CVE-2021-30140**	https://liquidfiles.com/support.html	A-LIQ-LIQU-280421/250
litespeedtech					
openlitespeed					
Improper Privilege Management	07-04-2021	9	Privilege Escalation in LiteSpeed Technologies OpenLiteSpeed web server version 1.7.8 allows attackers to gain root terminal access and execute commands on the host system. **CVE ID : CVE-2021-26758**	https://github.com/litespeedtech/openlitespeed/issues/217	A-LIT-OPEN-280421/251
magazinegerz_project					
magazinegerz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2021	4.3	Cross-site scripting vulnerability in MagazinegerZ v.1.01 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20684**	N/A	A-MAG-MAGA-280421/252
magnolia-cms					
magnolia_cms					
Improper Neutralization of Input	02-04-2021	4.3	Magnolia CMS from 6.1.3 to 6.2.3 contains a stored cross-site scripting (XSS)	https://git.magnolia-cms.com/	A-MAG-MAGN-280421/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability in the /magnoliaPublic/travel/members/login.html mgnlUserId parameter. **CVE ID : CVE-2021-25894**	projects/MODULES/repos/public-user-registration/commits/80c096c24d39ba2050b778e68ef838d79d4811dc, https://www.magnolia-cms.com/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	3.5	Magnolia CMS from 6.1.3 to 6.2.3 contains a stored cross-site scripting (XSS) vulnerability in the setText parameter of /magnoliaAuthor/.magnolia/. **CVE ID : CVE-2021-25893**	https://docs.magnolia-cms.com/product-docs/Releases/Release-notes-for-Magnolia-CMS-6.2.4.html#ReleasenotesforMagnoliaCMS6.2.4-Notablebugfixes, https://www.magnolia-cms.com	A-MAG-MAGN-280421/254
magpierss_project					
magpierss					
Improper Encoding or Escaping of	02-04-2021	7.5	Because of a incorrect escaped exec command in MagpieRSS in 0.72 in the	N/A	A-MAG-MAGP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output			/extlib/Snoopy.class.inc file, it is possible to add a extra command to the curl binary. This creates an issue on the /scripts/magpie_debug.php and /scripts/magpie_simple.php page that if you send a specific https url in the RSS URL field, you are able to execute arbitrary commands. **CVE ID : CVE-2021-28940**		280421/255
Server-Side Request Forgery (SSRF)	02-04-2021	5	Because of no validation on a curl command in MagpieRSS 0.72 in the /extlib/Snoopy.class.inc file, when you send a request to the /scripts/magpie_debug.php or /scripts/magpie_simple.php page, it's possible to request any internal page if you use a https request. **CVE ID : CVE-2021-28941**	N/A	A-MAG-MAGP-280421/256
marktext					
marktext					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	6.8	Mark Text through 0.16.3 allows attackers arbitrary command execution. This could lead to Remote Code Execution (RCE) by opening .md files containing a mutation Cross Site Scripting (XSS) payload. **CVE ID : CVE-2021-29996**	N/A	A-MAR-MARK-280421/257
matrix					
synapse					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-04-2021	4	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds. **CVE ID : CVE-2021-21394**	https://github.com/matrix-org/synapse/pull/9321, https://github.com/matrix-org/synapse/pull/9393, https://github.com/matrix-org/synapse/security/advisories/GHSA-w9fg-xffh-p362	A-MAT-SYNA-280421/258
Improper Input Validation	12-04-2021	4.3	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource	https://github.com/matrix-org/synapse/pull/9321, https://github.com/matrix-org/synapse/pull/9393, https://github.com/matrix-org/synap	A-MAT-SYNA-280421/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds. **CVE ID : CVE-2021-21393**	se/security/advisories/GHSA-jrh7-mhhx-6h88	
mcafee					
content_security_reporter					
Cleartext Transmission of Sensitive Information	15-04-2021	2.7	Cleartext Transmission of Sensitive Information vulnerability in the ePO Extension of McAfee Content Security Reporter (CSR) prior to 2.8.0 allows an ePO administrator to view the unencrypted password of the McAfee Web Gateway (MWG) or the password of the McAfee Web Gateway Cloud Server (MWGCS) read only user used to retrieve log files for analysis in CSR. **CVE ID : CVE-2021-23884**	https://kc.mcafee.com/corporate/index?page=content&id=SB10353	A-MCA-CONT-280421/260
data_loss_prevention_endpoint					
Improper Handling of Exceptional Conditions	15-04-2021	4.9	Denial of Service vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.100 allows a local, low privileged, attacker to cause a BSoD through suspending a process, modifying the processes memory and restarting it. This is triggered by the hdlphook	https://kc.mcafee.com/corporate/index?page=content&id=SB10354, https://kc.mcafee.com/corporate/index?page=cont	A-MCA-DATA-280421/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver reading invalid memory. **CVE ID : CVE-2021-23886**	ent&id=SB10357	
mediawiki					
mediawiki					
Incorrect Permission Assignment for Critical Resource	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.13 and 1.32.x through 1.35.x before 1.35.2. When using the MediaWiki API to "protect" a page, a user is currently able to protect to a higher level than they currently have permissions for. **CVE ID : CVE-2021-30152**	https://phabricator.wikimedia.org/T270713	A-MED-MEDI-280421/262
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	4.3	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. On Special:NewFiles, all the mediastatistics-header-* messages are output in HTML unescaped, leading to XSS. **CVE ID : CVE-2021-30154**	https://phabricator.wikimedia.org/T278014	A-MED-MEDI-280421/263
Missing Authorization	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. ContentModelChange does not check if a user has correct permissions to create and set the content model of a nonexistent page. **CVE ID : CVE-2021-30155**	https://phabricator.wikimedia.org/T270988	A-MED-MEDI-280421/264
Incorrect Permission Assignment for Critical	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2.	https://phabricator.wikimedia.org/T276	A-MED-MEDI-280421/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			Special:Contributions can leak that a "hidden" user exists. **CVE ID : CVE-2021-30156**	306	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	4.3	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. On ChangesList special pages such as Special:RecentChanges and Special:Watchlist, some of the rcfilters-filter-* label messages are output in HTML unescaped, leading to XSS. **CVE ID : CVE-2021-30157**	https://phabricator.wikimedia.org/T278058	A-MED-MEDI-280421/266
Improper Authentication	06-04-2021	5	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Blocked users are unable to use Special:ResetTokens. This has security relevance because a blocked user might have accidentally shared a token, or might know that a token has been compromised, and yet is not able to block any potential future use of the token by an unauthorized party. **CVE ID : CVE-2021-30158**	https://phabricator.wikimedia.org/T277009	A-MED-MEDI-280421/267
N/A	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Users can bypass intended restrictions on deleting pages in certain "fast double move" situations.	https://phabricator.wikimedia.org/T272386	A-MED-MEDI-280421/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MovePage::isValidMoveTarget() uses FOR UPDATE, but it's only called if Title::getArticleID() returns non-zero with no special flags. Next, MovePage::moveToInternal() will delete the page if getArticleID(READ_LATEST) is non-zero. Therefore, if the page is missing in the replica DB, isValidMove() will return true, and then moveToInternal() will unconditionally delete the page if it can be found in the master. **CVE ID : CVE-2021-30159**		
microfocus					
application_automation_tools					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Reflected XSS vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects all version 6.7 and earlier versions. **CVE ID : CVE-2021-22510**	https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-2175	A-MIC-APPL-280421/269
Improper Certificate Validation	08-04-2021	6.4	Improper Certificate Validation vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow unconditionally disabling of SSL/TLS certificates. **CVE ID : CVE-2021-22511**	https://www.jenkins.io/security/advisory/2021-04-07/#SECURITY-2176	A-MIC-APPL-280421/270
Cross-Site	08-04-2021	4.3	Cross-Site Request Forgery	https://w	A-MIC-APPL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			(CSRF) vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow form validation without permission checks. **CVE ID : CVE-2021-22512**	ww.jenkins.io/security/advisory/2021-04-07/#SECURITY-2132	280421/271
Missing Authorization	08-04-2021	4	Missing Authorization vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow access without permission checks. **CVE ID : CVE-2021-22513**	N/A	A-MIC-APPL-280421/272
netiq_advanced_authentication					
Improper Authentication	12-04-2021	6.5	Advanced Authentication versions prior to 6.3 SP4 have a potential broken authentication due to improper session management issue. **CVE ID : CVE-2021-22497**	https://www.netiq.com/documentation/advanced-authentication-63/advanced-authentication-releasenotes-634/data/advanced-authentication-releasenotes-	A-MIC-NETI-280421/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				634.html	
operations_agent					
Improper Privilege Management	13-04-2021	7.5	Escalation of privileges vulnerability in Micro Focus Operations Agent, affects versions 12.0x, 12.10, 12.11, 12.12, 12.14 and 12.15. The vulnerability could be exploited to escalate privileges and execute code under the account of the Operations Agent. **CVE ID : CVE-2021-22505**	https://softwaresupport.softwaregrp.com/doc/KM03792442	A-MIC-OPER-280421/274
operations_bridge_manager					
Improper Authentication	08-04-2021	7.5	Authentication bypass vulnerability in Micro Focus Operations Bridge Manager affects versions 2019.05, 2019.11, 2020.05 and 2020.10. The vulnerability could allow remote attackers to bypass user authentication and get unauthorized access. **CVE ID : CVE-2021-22507**	https://softwaresupport.softwaregrp.com/doc/KM03793283	A-MIC-OPER-280421/275
microsoft					
365_apps					
N/A	13-04-2021	6.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2021-28449**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28449	A-MIC-365_-280421/276
N/A	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is	https://portal.msrc.microsoft.	A-MIC-365_-280421/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-28454. **CVE ID : CVE-2021-28451**	com/en-US/security-guidance/advisory/CVE-2021-28451	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-04-2021	6.8	Microsoft Outlook Memory Corruption Vulnerability **CVE ID : CVE-2021-28452**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28452	A-MIC-365_-280421/278
Use After Free	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28451. **CVE ID : CVE-2021-28454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28454	A-MIC-365_-280421/279
N/A	13-04-2021	4.3	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2021-28456**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28456	A-MIC-365_-280421/280
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-365_-280421/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-28453	
azure_sphere					
N/A	13-04-2021	4.6	Azure Sphere Unsigned Code Execution Vulnerability **CVE ID : CVE-2021-28460**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28460	A-MIC-AZUR-280421/282
excel					
N/A	13-04-2021	6.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2021-28449**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28449	A-MIC-EXCE-280421/283
N/A	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28454. **CVE ID : CVE-2021-28451**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28451	A-MIC-EXCE-280421/284
N/A	13-04-2021	4.3	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2021-28456**	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-EXCE-280421/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-28456	
exchange_server					
Untrusted Search Path	08-04-2021	4.6	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges. **CVE ID : CVE-2021-3146**	https://professional.dolby.com/siteassets/pdfs/dolby-dax2-security-advisory-2021-04-07.pdf	A-MIC-EXCH-280421/286
N/A	13-04-2021	10	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28481, CVE-2021-28482, CVE-2021-28483. **CVE ID : CVE-2021-28480**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28480	A-MIC-EXCH-280421/287
N/A	13-04-2021	10	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28482, CVE-2021-28483. **CVE ID : CVE-2021-28481**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28481	A-MIC-EXCH-280421/288
N/A	13-04-2021	9	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28483. **CVE ID : CVE-2021-28482**	https://portal.msrc.microsoft.com/en-US/security-guidance/	A-MIC-EXCH-280421/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-28482	
N/A	13-04-2021	7.7	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28480, CVE-2021-28481, CVE-2021-28482. **CVE ID : CVE-2021-28483**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28483	A-MIC-EXCH-280421/290
ms-rest-nodeauth					
Improper Privilege Management	13-04-2021	6.8	Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28458**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28458	A-MIC-MS-R-280421/291
office					
N/A	13-04-2021	6.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2021-28449**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28449	A-MIC-OFFI-280421/292
N/A	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28454. **CVE ID : CVE-2021-28451**	https://portal.msrc.microsoft.com/en-US/security-guidance/	A-MIC-OFFI-280421/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-28451	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-04-2021	6.8	Microsoft Outlook Memory Corruption Vulnerability **CVE ID : CVE-2021-28452**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28452	A-MIC-OFFI-280421/294
Use After Free	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28451. **CVE ID : CVE-2021-28454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28454	A-MIC-OFFI-280421/295
N/A	13-04-2021	4.3	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2021-28456**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28456	A-MIC-OFFI-280421/296
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	A-MIC-OFFI-280421/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28453	
office_online_server					
N/A	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28454. **CVE ID : CVE-2021-28451**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28451	A-MIC-OFFI-280421/298
Use After Free	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28451. **CVE ID : CVE-2021-28454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28454	A-MIC-OFFI-280421/299
N/A	13-04-2021	4.3	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2021-28456**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28456	A-MIC-OFFI-280421/300
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28453	A-MIC-OFFI-280421/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
office_web_apps					
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28453	A-MIC-OFFI-280421/302
office_web_apps_server					
N/A	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28454. **CVE ID : CVE-2021-28451**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28451	A-MIC-OFFI-280421/303
Use After Free	13-04-2021	6.8	Microsoft Excel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28451. **CVE ID : CVE-2021-28454**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28454	A-MIC-OFFI-280421/304
N/A	13-04-2021	4.3	Microsoft Excel Information Disclosure Vulnerability **CVE ID : CVE-2021-28456**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28456	A-MIC-OFFI-280421/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28453	A-MIC-OFFI-280421/306
outlook					
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-04-2021	6.8	Microsoft Outlook Memory Corruption Vulnerability **CVE ID : CVE-2021-28452**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28452	A-MIC-OUTL-280421/307
raw_image_extension					
N/A	13-04-2021	6.8	Raw Image Extension Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28468. **CVE ID : CVE-2021-28466**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28466	A-MIC-RAW_-280421/308
Access of Resource Using Incompatible Type ('Type Confusion')	13-04-2021	6.8	Raw Image Extension Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28466. **CVE ID : CVE-2021-28468**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28468	A-MIC-RAW_-280421/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sharepoint_foundation					
N/A	13-04-2021	4	Microsoft SharePoint Denial of Service Update **CVE ID : CVE-2021-28450**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28450	A-MIC-SHAR-280421/310
sharepoint_server					
N/A	13-04-2021	4	Microsoft SharePoint Denial of Service Update **CVE ID : CVE-2021-28450**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28450	A-MIC-SHAR-280421/311
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28453	A-MIC-SHAR-280421/312
team_foundation_server					
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability **CVE ID : CVE-2021-27067**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	A-MIC-TEAM-280421/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				27067	
visual_c++					
Untrusted Search Path	08-04-2021	4.6	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges. **CVE ID : CVE-2021-3146**	https://professional.dolby.com/siteassets/pdfs/dolby-dax2-security-advisory-2021-04-07.pdf	A-MIC-VISU-280421/314
visual_studio					
Untrusted Search Path	08-04-2021	4.6	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges. **CVE ID : CVE-2021-3146**	https://professional.dolby.com/siteassets/pdfs/dolby-dax2-security-advisory-2021-04-07.pdf	A-MIC-VISU-280421/315
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322. **CVE ID : CVE-2021-28313**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28313	A-MIC-VISU-280421/316
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	A-MIC-VISU-280421/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28321	
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322	A-MIC-VISU-280421/318
visual_studio_.net					
Untrusted Search Path	08-04-2021	4.6	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges. **CVE ID : CVE-2021-3146**	https://professional.dolby.com/siteassets/pdfs/dolby-dax2-security-advisory-2021-04-07.pdf	A-MIC-VISU-280421/319
visual_studio_2017					
Improper Privilege Management	13-04-2021	4.6	Visual Studio Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27064**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27064	A-MIC-VISU-280421/320
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322. **CVE ID : CVE-2021-28313**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	A-MIC-VISU-280421/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28313	
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321	A-MIC-VISU-280421/322
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322	A-MIC-VISU-280421/323
visual_studio_2019					
Improper Privilege Management	13-04-2021	4.6	Visual Studio Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27064**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27064	A-MIC-VISU-280421/324
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322. **CVE ID : CVE-2021-28313**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28313	A-MIC-VISU-280421/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321	A-MIC-VISU-280421/326
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322	A-MIC-VISU-280421/327
visual_studio_code					
N/A	13-04-2021	6.8	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28469, CVE-2021-28473, CVE-2021-28475, CVE-2021-28477. **CVE ID : CVE-2021-28457**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28457	A-MIC-VISU-280421/328
N/A	13-04-2021	6.8	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28473, CVE-2021-28475, CVE-2021-28477. **CVE ID : CVE-2021-28469**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28469	A-MIC-VISU-280421/329
N/A	13-04-2021	6.8	Remote Development	https://po	A-MIC-VISU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Extension for Visual Studio Code Remote Code Execution Vulnerability **CVE ID : CVE-2021-28471**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28471	280421/330
N/A	13-04-2021	6.8	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28475, CVE-2021-28477. **CVE ID : CVE-2021-28473**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28473	A-MIC-VISU-280421/331
N/A	13-04-2021	6.8	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28473, CVE-2021-28477. **CVE ID : CVE-2021-28475**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28475	A-MIC-VISU-280421/332
N/A	13-04-2021	6.8	Visual Studio Code Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28457, CVE-2021-28469, CVE-2021-28473, CVE-2021-28475. **CVE ID : CVE-2021-28477**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28477	A-MIC-VISU-280421/333
visual_studio_code_github_pull_requests_and_issues					
N/A	13-04-2021	6.8	Visual Studio Code GitHub Pull Requests and Issues	https://portal.msrc.	A-MIC-VISU-280421/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Extension Remote Code Execution Vulnerability **CVE ID : CVE-2021-28470**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-28470	
visual_studio_code_kubernetes_tools					
N/A	13-04-2021	6.8	Visual Studio Code Kubernetes Tools Remote Code Execution Vulnerability **CVE ID : CVE-2021-28448**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28448	A-MIC-VISU-280421/335
vp9_video_extensions					
N/A	13-04-2021	6.8	VP9 Video Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2021-28464**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28464	A-MIC-VP9_-280421/336
vscode-maven					
N/A	13-04-2021	6.8	Visual Studio Code Maven for Java Extension Remote Code Execution Vulnerability **CVE ID : CVE-2021-28472**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28472	A-MIC-VSCO-280421/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
word					
N/A	13-04-2021	6.8	Microsoft Word Remote Code Execution Vulnerability **CVE ID : CVE-2021-28453**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28453	A-MIC-WORD-280421/338
mirahezebots					
sopel-channelmgnt					
Improper Input Validation	09-04-2021	5.5	sopel-channelmgnt is a channelmgnt plugin for sopel. In versions prior to 2.0.1, on some IRC servers, restrictions around the removal of the bot using the kick/kickban command could be bypassed when kicking multiple users at once. We also believe it may have been possible to remove users from other channels but due to the wonder that is IRC and following RfCs, We have no POC for that. Freenode is not affected. This is fixed in version 2.0.1. As a workaround, do not use this plugin on networks where TARGMAX > 1. **CVE ID : CVE-2021-21431**	https://github.com/MirahezeBots/sopel-channelmgnt/security/advisories/GHSA-23c7-6444-399m, https://github.com/MirahezeBots/sopel-channelmgnt/commit/7c96d400358221e59135f0a0be0744f3fad73856	A-MIR-SOPE-280421/339
mitake					
smart_stock_selection					
Improper Authentication	08-04-2021	6.4	Mitake smart stock selection system contains a broken authentication vulnerability. By	N/A	A-MIT-SMAR-280421/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulating the parameters in the URL, remote attackers can gain the privileged permissions to access transaction record, and fraudulent trading without login. **CVE ID : CVE-2021-28174**		
mongo-express_project					
mongo-express					
Improper Check for Unusual or Exceptional Conditions	13-04-2021	5	All versions of package mongo-express are vulnerable to Denial of Service (DoS) when exporting an empty collection as CSV, due to an unhandled exception, leading to a crash. **CVE ID : CVE-2021-23372**	N/A	A-MON-MONG-280421/341
mongodb					
compass					
Improper Privilege Management	06-04-2021	4.6	A malicious 3rd party with local access to the Windows machine where MongoDB Compass is installed can execute arbitrary software with the privileges of the user who is running MongoDB Compass. This issue affects: MongoDB Inc. MongoDB Compass 1.x version 1.3.0 on Windows and later versions; 1.x versions prior to 1.25.0 on Windows. **CVE ID : CVE-2021-20334**	https://jira.mongodb.org/browse/COMPASS-4510	A-MON-COMP-280421/342
n5_upload_form_project					
n5_upload_form					
Unrestricted Upload of File	12-04-2021	7.5	The N5 Upload Form WordPress plugin through	https://wpscan.com	A-N5_-N5_U-280421/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Dangerous Type			1.0 suffers from an arbitrary file upload issue in page where a Form from the plugin is embed, as any file can be uploaded. The uploaded filename might be hard to guess as it's generated with md5(uniqid(rand())), however, in the case of misconfigured servers with Directory listing enabled, accessing it is trivial. **CVE ID : CVE-2021-24223**	/vulnerability/d7a72183-0cd1-45de-b98b-2e295b27e5db	
nagios					
network_analyzer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-04-2021	7.5	SQL injection vulnerability in Nagios Network Analyzer before 2.4.3 via the o[col] parameter to api/checks/read/. **CVE ID : CVE-2021-28925**	https://www.nagios.com/downloads/nagios-network-analyzer/change-log/	A-NAG-NETW-280421/344
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	Self Authenticated XSS in Nagios Network Analyzer before 2.4.2 via the nagiosna/groups/queries page. **CVE ID : CVE-2021-28924**	https://www.nagios.com/downloads/nagios-network-analyzer/change-log/	A-NAG-NETW-280421/345
net					
Incorrect Authorization	06-04-2021	5	The Net::Netmask module before 2.0000 for Perl does not properly consider extraneous zero characters at the beginning of an IP	N/A	A-NET--280421/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses. **CVE ID : CVE-2021-29424**		
netmask_project					
netmask					
Improper Input Validation	01-04-2021	6.4	Improper input validation of octal strings in netmask npm package v1.0.6 and below allows unauthenticated remote attackers to perform indeterminate SSRF, RFI, and LFI attacks on many of the dependent packages. A remote unauthenticated attacker can bypass packages relying on netmask to filter IPs and reach critical VPN or LAN hosts. **CVE ID : CVE-2021-28918**	N/A	A-NET-NETM-280421/347
nettle_project					
nettle					
Use of a Broken or Risky Cryptographic Algorithm	05-04-2021	6.8	A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure	https://bugzilla.redhat.com/show_bug.cgi?id=1942533	A-NET-NETT-280421/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-20305**		
never5					
related_posts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	Unvalidated input and lack of output encoding within the Related Posts for WordPress plugin before 2.0.4 lead to a Reflected Cross-Site Scripting (XSS) vulnerability within the 'lang' GET parameter while editing a post, triggered when users with the capability of editing posts access a malicious URL. **CVE ID : CVE-2021-24180**	https://wpscan.com/vulnerability/7593d5c8-cbc2-4469-b36b-5d4fb6d49718	A-NEV-RELA-280421/349
nextcloud					
desktop					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-04-2021	6.8	Nextcloud Desktop Client prior to 3.1.3 is vulnerable to resource injection by way of missing validation of URLs, allowing a malicious server to execute remote commands. User interaction is needed for exploitation. **CVE ID : CVE-2021-22879**	https://nextcloud.com/security/advisory/?id=NC-SA-2021-008, https://github.com/nextcloud/desktop/pull/2906	A-NEX-DESK-280421/350
nextcloud/dialogs_project					
nextcloud/dialogs					
Improper Neutralization of Input	13-04-2021	4.3	The Nextcloud dialogs library (npm package @nextcloud/dialogs)	https://github.com/nextcloud	A-NEX-NEXT-280421/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			before 3.1.2 insufficiently escaped text input passed to a toast. If your application displays toasts with user-supplied input, this could lead to a XSS vulnerability. The vulnerability has been patched in version 3.1.2 If you need to display HTML in the toast, explicitly pass the `options.isHTML` config flag. **CVE ID : CVE-2021-29438**	/nextcloud-dialogs/security/advisories/GHSA-g3fq-3v3g-mh32	
ninjaforms					
ninja_forms					
Exposure of Sensitive Information to an Unauthorized Actor	05-04-2021	6.5	The AJAX action, wp_ajax_ninja_forms_send wp_remote_install_handler, did not have a capability check on it, nor did it have any nonce protection, therefore making it possible for low-level users, such as subscribers, to install and activate the SendWP Ninja Forms Contact Form â€“ The Drag and Drop Form Builder for WordPress WordPress plugin before 3.4.34 and retrieve the client_secret key needed to establish the SendWP connection while also installing the SendWP plugin. **CVE ID : CVE-2021-24163**	https://wpscan.com/vulnerability/55fde9fa-f6cd-4546-bee8-4acc628251c2	A-NIN-NINJ-280421/352
Exposure of Sensitive Information to an Unauthorized	05-04-2021	4	In the Ninja Forms Contact Form WordPress plugin before 3.4.34.1, low-level users, such as subscribers, were able to trigger the	https://wpscan.com/vulnerability/dfa32afa-c6de-	A-NIN-NINJ-280421/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Actor			action, wp_ajax_nf_oauth, and retrieve the connection url needed to establish a connection. They could also retrieve the client_id for an already established OAuth connection. **CVE ID : CVE-2021-24164**	4237-a9f2-709843dcda89	
URL Redirection to Untrusted Site ('Open Redirect')	05-04-2021	5.8	In the Ninja Forms Contact Form WordPress plugin before 3.4.34, the wp_ajax_nf_oauth_connect AJAX action was vulnerable to open redirect due to the use of a user supplied redirect parameter and no protection in place. **CVE ID : CVE-2021-24165**	https://wpscan.com/vulnerability/6147acf5-e43f-47e6-ab56-c9c8be584818	A-NIN-NINJ-280421/354
Cross-Site Request Forgery (CSRF)	05-04-2021	5.8	The wp_ajax_nf_oauth_disconnect from the Ninja Forms Contact Form – The Drag and Drop Form Builder for WordPress WordPress plugin before 3.4.34 had no nonce protection making it possible for attackers to craft a request to disconnect a site's OAuth connection. **CVE ID : CVE-2021-24166**	https://wpscan.com/vulnerability/b531fb65-a8ff-4150-a9a1-2a62a3c00bd6	A-NIN-NINJ-280421/355
node-etsy-client_project					
node-etsy-client					
Exposure of Sensitive Information to an Unauthorized Actor	01-04-2021	4	node-etsy-client is a NodeJs Etsy ReST API Client. Applications that are using node-etsy-client and reporting client error to the end user will offer api key value too This is fixed in node-etsy-client v0.3.0 and	https://github.com/creharmony/node-etsy-client/commit/b4beb8ef0803	A-NOD-NODE-280421/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			later. **CVE ID : CVE-2021-21421**	66c1a87dbf9e163051a446acaa7d, https://github.com/creharmony/node-etsy-client/security/advisories/GHSA-xw22-wv29-3299	
ocproducts					
composr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	4.3	Composr 10.0.36 allows XSS in an XML script. **CVE ID : CVE-2021-30150**	https://gitlab.com/composr-foundation/composr/commit/833a06466	A-OCP-COMP-280421/357
Unrestricted Upload of File with Dangerous Type	06-04-2021	7.5	Composr 10.0.36 allows upload and execution of PHP files. **CVE ID : CVE-2021-30149**	https://gitlab.com/composr-foundation/composr/commit/a71c44e03	A-OCP-COMP-280421/358
okta					
access_gateway					
Improper Neutralization of Special Elements used in an OS Command ('OS	02-04-2021	8.7	A command injection vulnerability in the cookieDomain and relayDomain parameters of Okta Access Gateway before 2020.9.3 allows attackers (with admin	https://www.okta.com/security-advisories/cve-2021-	A-OKT-ACCE-280421/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			access to the Okta Access Gateway UI) to execute OS commands as a privileged system account. **CVE ID : CVE-2021-28113**	28113	
online_reviewer_system_project					
online_reviewer_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-04-2021	7.5	Online Reviewer System 1.0 contains a SQL injection vulnerability through authentication bypass, which may lead to a reverse shell upload. **CVE ID : CVE-2021-27130**	N/A	A-ONL-ONLI-280421/360
openexr					
openexr					
NULL Pointer Dereference	01-04-2021	5	A flaw was found in OpenEXR in versions before 3.0.0-beta. A crafted input file supplied by an attacker, that is processed by the Dwa decompression functionality of OpenEXR's IlmImf library, could cause a NULL pointer dereference. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-20296**	https://bugzilla.redhat.com/show_bug.cgi?id=1939141, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=24854	A-OPE-OPEN-280421/361
outer_cgi_project					
outer_cgi					
Improper Restriction of Operations within the Bounds of a Memory	07-04-2021	7.5	An issue was discovered in the outer_cgi crate before 0.2.1 for Rust. A user-provided Read instance receives an uninitialized memory buffer from	N/A	A-OUT-OUTE-280421/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			KeyValueReader. **CVE ID : CVE-2021-30454**		
outsystems					
lifetime_management_console					
Server-Side Request Forgery (SSRF)	12-04-2021	5	The ECT Provider component in OutSystems Platform Server 10 before 10.0.1104.0 and 11 before 11.9.0 (and LifeTime management console before 11.7.0) allows SSRF for arbitrary outbound HTTP requests. **CVE ID : CVE-2021-29357**	https://success.outsystems.com/Support/Security/Vulnerabilities/Vulnerability_RTAF-2226	A-OUT-LIFE-280421/363
outsystems					
Server-Side Request Forgery (SSRF)	12-04-2021	5	The ECT Provider component in OutSystems Platform Server 10 before 10.0.1104.0 and 11 before 11.9.0 (and LifeTime management console before 11.7.0) allows SSRF for arbitrary outbound HTTP requests. **CVE ID : CVE-2021-29357**	https://success.outsystems.com/Support/Security/Vulnerabilities/Vulnerability_RTAF-2226	A-OUT-OUTS-280421/364
platform_server					
Server-Side Request Forgery (SSRF)	12-04-2021	5	The ECT Provider component in OutSystems Platform Server 10 before 10.0.1104.0 and 11 before 11.9.0 (and LifeTime management console before 11.7.0) allows SSRF for arbitrary outbound HTTP requests. **CVE ID : CVE-2021-29357**	https://success.outsystems.com/Support/Security/Vulnerabilities/Vulnerability_RTAF-2226	A-OUT-PLAT-280421/365
papoo					
papoo					
Cross-Site	13-04-2021	6.8	Certain Papoo products are	https://pa	A-PAP-PAPO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			affected by: Cross Site Request Forgery (CSRF) in the admin interface. This affects Papoo CMS Light through 21.02 and Papoo CMS Pro through 6.0.1. The impact is: gain privileges (remote). **CVE ID : CVE-2021-29054**	cketstorm security.com/files/162077/Papoo-CMS-Cross-Site-Request-Forgery.html, https://www.papoo.de/achtung---sicherheitsfeature-bitte-aktivieren.html, https://github.com/raginx/security/blob/main/rADV-2021-01.txt	280421/366
parse_duration_project					
parse_duration					
Uncontrolled Resource Consumption	01-04-2021	5	An issue was discovered in the parse_duration crate through 2021-03-18 for Rust. It allows attackers to cause a denial of service (CPU and memory consumption) via a duration string with a large exponent. **CVE ID : CVE-2021-29932**	https://rustsec.org/advisories/RUSTSEC-2021-0041.html	A-PAR-PARS-280421/367
patreon					
patreon_wordpress					
Cross-Site Request Forgery	12-04-2021	4.3	The Jetpack Scan team identified a Cross-Site Request Forgery	https://wpscan.com/vulnerabi	A-PAT-PATR-280421/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			vulnerability in the Patreon WordPress plugin before 1.7.0, allowing attackers to make a logged administrator disconnect the site from Patreon by visiting a specially crafted link. **CVE ID : CVE-2021-24231**	lity/f8ab6855-a319-47ac-82fb-58b181e77500	
Cross-Site Request Forgery (CSRF)	12-04-2021	5.8	The Jetpack Scan team identified a Cross-Site Request Forgery vulnerability in the Patreon WordPress plugin before 1.7.0, allowing attackers to make a logged in user overwrite or create arbitrary user metadata on the victim's account once visited. If exploited, this bug can be used to overwrite the "wp_capabilities" meta, which contains the affected user account's roles and privileges. Doing this would essentially lock them out of the site, blocking them from accessing paid content. **CVE ID : CVE-2021-24230**	https://wpscan.com/vulnerability/2deefa2d-3043-42e5-afef-a42c37703531	A-PAT-PATR-280421/369
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	6.8	The Jetpack Scan team identified a Reflected Cross-Site Scripting via the patreon_save_attachment_patreon_level AJAX action of the Patreon WordPress plugin before 1.7.2. This AJAX hook is used to update the pledge level required by Patreon subscribers to access a given attachment. This	https://wpscan.com/vulnerability/001755c4-add3-4566-a022-ab1f83546c1f	A-PAT-PATR-280421/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			action is accessible for user accounts with the 'manage_options' privilege (i.e.., only administrators). Unfortunately, one of the parameters used in this AJAX endpoint is not sanitized before being printed back to the user, so the risk it represents is the same as the previous XSS vulnerability. **CVE ID : CVE-2021-24229**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	6.8	The Jetpack Scan team identified a Reflected Cross-Site Scripting in the Login Form of the Patreon WordPress plugin before 1.7.2. The WordPress login form (wp-login.php) is hooked by the plugin and offers to allow users to authenticate on the site using their Patreon account. Unfortunately, some of the error logging logic behind the scene allowed user-controlled input to be reflected on the login page, unsanitized. **CVE ID : CVE-2021-24228**	https://wpscan.com/vulnerability/7a5fadb1-3f1c-4779-8ff6-356fccb5269b	A-PAT-PATR-280421/371
Exposure of Sensitive Information to an Unauthorized Actor	12-04-2021	5	The Jetpack Scan team identified a Local File Disclosure vulnerability in the Patreon WordPress plugin before 1.7.0 that could be abused by anyone visiting the site. Using this attack vector, an attacker could leak important internal files like wp-config.php, which contains database credentials and	https://wpscan.com/vulnerability/f62df02d-7678-440f-84a1-ddbf09364016	A-PAT-PATR-280421/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic keys used in the generation of nonces and cookies. **CVE ID : CVE-2021-24227**		
pega					
infinity					
N/A	01-04-2021	4	Misconfiguration of the Pega Chat Access Group portal in Pega platform 7.4.0 - 8.5.x could lead to unintended data exposure. **CVE ID : CVE-2021-27653**	https://collaborate.pega.com/discussion/pega-security-advisory-%E2%80%93-b21	A-PEG-INFI-280421/373
perforce					
helix_alm					
Improper Restriction of XML External Entity Reference	13-04-2021	6.4	XML External Entity Resolution (XXE) in Helix ALM. The XML Import functionality of the Administration console in Perforce Helix ALM 2020.3.1 Build 22 accepts XML input data that is parsed by insecurely configured software components, leading to XXE attacks. **CVE ID : CVE-2021-29997**	N/A	A-PER-HELI-280421/374
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	13-04-2021	4	The XML Import functionality of the Administration console in Perforce Helix ALM 2020.3.1 Build 22 accepts XML input data that is parsed by insecurely configured software components, leading to XXE attacks.	N/A	A-PER-HELI-280421/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28973		
phpgurukul_beauty_parlour_management_system_project					
phpgurukul_beauty_parlour_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-04-2021	3.5	Cross Site Scripting (XSS) in the "add-services.php" component of PHPGurukul Beauty Parlour Management System v1.0 allows remote attackers to execute arbitrary code by injecting arbitrary HTML into the "sername" parameter. **CVE ID : CVE-2021-27544**	N/A	A-PHP-PHPG-280421/376
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-04-2021	4	SQL Injection in the "add-services.php" component of PHPGurukul Beauty Parlour Management System v1.0 allows remote attackers to obtain sensitive database information by injecting SQL commands into the "sername" parameter. **CVE ID : CVE-2021-27545**	N/A	A-PHP-PHPG-280421/377
phpnuke					
php-nuke					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-04-2021	7.5	There is a SQL Injection vulnerability in PHP-Nuke 8.3.3 in the User Registration section, leading to remote code execution. This occurs because the U.S. state is not validated to be two letters, and the OrderBy field is not validated to be one of LASTNAME, CITY, or STATE. **CVE ID : CVE-2021-30177**	N/A	A-PHP-PHP--280421/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
phpseclib					
phpseclib					
Improper Verification of Cryptographic Signature	06-04-2021	5	phpseclib before 2.0.31 and 3.x before 3.0.7 mishandles RSA PKCS#1 v1.5 signature verification. **CVE ID : CVE-2021-30130**	https://github.com/phpseclib/phpseclib/releases/tag/2.0.31, https://github.com/phpseclib/phpseclib/releases/tag/3.0.7	A-PHP-PHPS-280421/379
pikepdf_project					
pikepdf					
Improper Restriction of XML External Entity Reference	01-04-2021	5	models/metadata.py in the pikepdf package 1.3.0 through 2.9.2 for Python allows XXE when parsing XMP metadata entries. **CVE ID : CVE-2021-29421**	https://github.com/pikepdf/pikepdf/commit/3f38f73218e5e782fe411ccbb3b44a793c0b343a	A-PIK-PIKE-280421/380
piwigo					
piwigo					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2021	6.5	SQL injection exists in Piwigo before 11.4.0 via the language parameter to admin.php?page=languages. **CVE ID : CVE-2021-27973**	https://github.com/Piwigo/Piwigo/issues/1352	A-PIW-PIWI-280421/381
pomerium					
pomerium					
URL	02-04-2021	5.8	Pomerium before 0.13.4	https://git	A-POM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirection to Untrusted Site ('Open Redirect')			has an Open Redirect (issue 1 of 2). **CVE ID : CVE-2021-29651**	hub.com/pomerium/pomerium/security/advisories/GHSA-35vc-w93w-75c2	POME-280421/382
URL Redirection to Untrusted Site ('Open Redirect')	02-04-2021	5.8	Pomerium from version 0.10.0-0.13.3 has an Open Redirect in the user sign-in/out process **CVE ID : CVE-2021-29652**	https://github.com/pomerium/pomerium/security/advisories/GHSA-fv82-r8qv-ch4v	A-POM-POME-280421/383
posimyth					
the_plus_addons_for_elementor					
Improper Authentication	05-04-2021	7.5	The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.7 was being actively exploited to by malicious actors to bypass authentication, allowing unauthenticated users to log in as any user (including admin) by just providing the related username, as well as create accounts with arbitrary roles, such as admin. These issues can be exploited even if registration is disabled, and the Login widget is not active. **CVE ID : CVE-2021-24175**	https://wpscan.com/vulnerability/c311feef-7041-4c21-9525-132b9bd32f89	A-POS-THE_-280421/384
postcss					
postcss					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	12-04-2021	5	The package postcss from 7.0.0 and before 8.2.10 are vulnerable to Regular Expression Denial of Service (ReDoS) during source map parsing. **CVE ID : CVE-2021-23368**	https://github.com/postcss/postcss/commit/8682b1e4e328432ba692bed52326e84439cec9e4, https://github.com/postcss/postcss/commit/b6f3e4d5a8d7504d553267f80384373af3a3dec5	A-POS-POST-280421/385
postgresql					
postgresql					
Generation of Error Message Containing Sensitive Information	01-04-2021	3.5	An information leak was discovered in postgresql in versions before 13.2, before 12.6 and before 11.11. A user having UPDATE permission but not SELECT permission to a particular column could craft queries which, under some circumstances, might disclose values from that column in error messages. An attacker could use this flaw to obtain information stored in a column they are allowed to write but not read. **CVE ID : CVE-2021-3393**	N/A	A-POS-POST-280421/386
priority-software					
priority_enterprise_management_system					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2021	4.3	Cross Site Scripting (XSS) in the "Reset Password" page form of Priority Enterprise Management System v8.00 allows attackers to execute javascript on behalf of the victim by sending a malicious URL or directing the victim to a malicious site. **CVE ID : CVE-2021-26832**	N/A	A-PRI-PRIO-280421/387
projen_project					
projen					
Exposure of Version-Control Repository to an Unauthorized Control Sphere	06-04-2021	5.5	`projen` is a project generation tool that synthesizes project configuration files such as `package.json`, `tsconfig.json`, `.gitignore`, GitHub Workflows, `eslint`, `jest`, and more, from a well-typed definition written in JavaScript. Users of projen's `NodeProject` project type (including any project type derived from it) include a `.github/workflows/rebuild-bot.yml` workflow that may allow any GitHub user to trigger execution of un-trusted code in the context of the "main" repository (as opposed to that of a fork). In some situations, such untrusted code may potentially be able to commit to the "main" repository. The rebuild-bot workflow is triggered by comments including `@projen rebuild` on pull-	https://github.com/projen/projen/security/advisories/GHSA-gg2g-m5wc-vccq, https://github.com/projen/projen/commit/36030c6a4b1acd0054673322612e7c70e9446643	A-PRO-PROJ-280421/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request to trigger a re-build of the projen project, and updating the pull request with the updated files. This workflow is triggered by an `issue_comment` event, and thus always executes with a `GITHUB_TOKEN` belonging to the repository into which the pull-request is made (this is in contrast with workflows triggered by `pull_request` events, which always execute with a `GITHUB_TOKEN` belonging to the repository from which the pull-request is made). Repositories that do not have branch protection configured on their default branch (typically `main` or `master`) could possibly allow an untrusted user to gain access to secrets configured on the repository (such as NPM tokens, etc). Branch protection prohibits this escalation, as the managed `GITHUB_TOKEN` would not be able to modify the contents of a protected branch and affected workflows must be defined on the default branch. **CVE ID : CVE-2021-21423**		
proofpoint					
insider_threat_management					
Missing Authorization	06-04-2021	5.5	The Proofpoint Insider Threat Management Server (formerly ObserveIT	https://www.proofpoint.com/	A-PRO-INSI-280421/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server) is missing an authorization check on several pages in the Web Console. This enables a view-only user to change any configuration setting and delete any registered agents. All versions before 7.11.1 are affected. **CVE ID : CVE-2021-27900**	us/security/security-advisories/pfpt-sa-2021-0005	
Improper Certificate Validation	06-04-2021	5.8	The Proofpoint Insider Threat Management Agents (formerly ObserveIT Agent) for MacOS and Linux perform improper validation of the ITM Server's certificate, which enables a remote attacker to intercept and alter these communications using a man-in-the-middle attack. All versions before 7.11.1 are affected. Agents for Windows and Cloud are not affected. **CVE ID : CVE-2021-27899**	https://www.proofpoint.com/us/security/security-advisories/pfpt-sa-2021-0004	A-PRO-INSI-280421/390
Improper Restriction of XML External Entity Reference	06-04-2021	6.5	The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) is vulnerable to XML external entity (XXE) injection in the Web Console. The vulnerability requires admin user privileges and knowledge of the XML file's encryption key to successfully exploit. All versions before 7.11 are affected. **CVE ID : CVE-2021-22158**	https://www.proofpoint.com/us/security/security-advisories/pfpt-sa-2021-0003	A-PRO-INSI-280421/391
Improper Neutralizatio	06-04-2021	4.3	Proofpoint Insider Threat Management Server	https://www.proofp	A-PRO-INSI-280421/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			(formerly ObserveIT Server) before 7.11.1 allows stored XSS. **CVE ID : CVE-2021-22157**	oint.com/us/security/security-advisories/pfpt-sa-2021-0002	
qnap					
surveillance_station					
Out-of-bounds Write	14-04-2021	7.5	A stack-based buffer overflow vulnerability has been reported to affect QNAP NAS devices running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. QNAP have already fixed this vulnerability in the following versions: Surveillance Station 5.1.5.4.3 (and later) for ARM CPU NAS (64bit OS) and x86 CPU NAS (64bit OS) Surveillance Station 5.1.5.3.3 (and later) for ARM CPU NAS (32bit OS) and x86 CPU NAS (32bit OS) **CVE ID : CVE-2021-28797**	https://www.qnap.com/en/security-advisory/qsa-21-07	A-QNA-SURV-280421/393
rangerstudio					
directus					
Unrestricted Upload of File with Dangerous Type	07-04-2021	6.5	Directus 8 before 8.8.2 allows remote authenticated users to execute arbitrary code because file-upload permissions include the ability to upload a .php file to the main upload directory and/or upload a	N/A	A-RAN-DIRE-280421/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			.php file and a .htaccess file to a subdirectory. Exploitation succeeds only for certain installations with the Apache HTTP Server and the local-storage driver (e.g., when the product was obtained from hub.docker.com). **CVE ID : CVE-2021-29641**		
redhat					
ansible					
Insertion of Sensitive Information into Log File	01-04-2021	2.1	A flaw was found in several ansible modules, where parameters containing credentials, such as secrets, were being logged in plain-text on managed nodes, as well as being made visible on the controller node when run in verbose mode. These parameters were not protected by the no_log feature. An attacker can take advantage of this information to steal those credentials, provided when they have access to the log files containing them. The highest threat from this vulnerability is to data confidentiality. This flaw affects Red Hat Ansible Automation Platform in versions before 1.2.2 and Ansible Tower in versions before 3.8.2. **CVE ID : CVE-2021-3447**	https://bugzilla.redhat.com/show_bug.cgi?id=1939349	A-RED-ANSI-280421/395
ansible_tower					
Insertion of Sensitive Information	01-04-2021	2.1	A flaw was found in several ansible modules, where parameters containing	https://bugzilla.redhat.com/sh	A-RED-ANSI-280421/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
into Log File			credentials, such as secrets, were being logged in plain-text on managed nodes, as well as being made visible on the controller node when run in verbose mode. These parameters were not protected by the no_log feature. An attacker can take advantage of this information to steal those credentials, provided when they have access to the log files containing them. The highest threat from this vulnerability is to data confidentiality. This flaw affects Red Hat Ansible Automation Platform in versions before 1.2.2 and Ansible Tower in versions before 3.8.2. **CVE ID : CVE-2021-3447**	ow_bug.cgi?id=1939349	
openshift_container_platform					
Improper Locking	01-04-2021	7.1	A deadlock vulnerability was found in 'github.com/containers/storage' in versions before 1.28.1. When a container image is processed, each layer is unpacked using `tar`. If one of those layers is not a valid `tar` archive this causes an error leading to an unexpected situation where the code indefinitely waits for the tar unpacked stream, which never finishes. An attacker could use this vulnerability to craft a malicious image, which when downloaded and stored by an	https://bugzilla.redhat.com/show_bug.cgi?id=1939485	A-RED-OPEN-280421/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application using containers/storage, would then cause a deadlock leading to a Denial of Service (DoS). **CVE ID : CVE-2021-20291**		
satellite					
Exposure of Sensitive Information to an Unauthorized Actor	08-04-2021	6.5	A flaw was found in Red Hat Satellite in tfm-rubygem-foreman_azure_rm in versions before 2.2.0. A credential leak was identified which will expose Azure Resource Manager's secret key through JSON of the API output. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3413**	N/A	A-RED-SATE-280421/398
software_collections					
Generation of Error Message Containing Sensitive Information	01-04-2021	3.5	An information leak was discovered in postgresql in versions before 13.2, before 12.6 and before 11.11. A user having UPDATE permission but not SELECT permission to a particular column could craft queries which, under some circumstances, might disclose values from that column in error messages. An attacker could use this flaw to obtain information stored in a column they are allowed to write but not read.	N/A	A-RED-SOFT-280421/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3393		
redmine					
redmine					
Exposure of Sensitive Information to an Unauthorized Actor	06-04-2021	5	Redmine before 4.0.8 and 4.1.x before 4.1.2 allows attackers to discover the names of private projects if issue-journal details exist that have changes to project_id values. **CVE ID : CVE-2021-30163**	N/A	A-RED-REDM-280421/400
N/A	06-04-2021	7.5	Redmine before 4.0.8 and 4.1.x before 4.1.2 allows attackers to bypass the add_issue_notes permission requirement by leveraging the Issues API. **CVE ID : CVE-2021-30164**	N/A	A-RED-REDM-280421/401
remoteclinic					
remoteclinic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the Full Name field on register-patient.php. **CVE ID : CVE-2021-30030**	N/A	A-REM-REMO-280421/402
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the Symptons field on patients/register-report.php. **CVE ID : CVE-2021-30034**	N/A	A-REM-REMO-280421/403
Improper Neutralization of Input During Web	13-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Fever" or "Blood Pressure" field on the	N/A	A-REM-REMO-280421/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			patients/register-report.php. **CVE ID : CVE-2021-30039**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Clinic Name", "Clinic Address", "Clinic City", or "Clinic Contact" field on clinics/register.php **CVE ID : CVE-2021-30042**	N/A	A-REM-REMO-280421/405
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the First Name or Last Name field on staff/register.php. **CVE ID : CVE-2021-30044**	N/A	A-REM-REMO-280421/406
reorder_project					
reorder					
Out-of-bounds Write	01-04-2021	7.5	An issue was discovered in the reorder crate through 2021-02-24 for Rust. swap_index has an out-of-bounds write if an iterator returns a len() that is too small. **CVE ID : CVE-2021-29941**	https://rustsec.org/advisories/RUSTSEC-2021-0050.html	A-REO-REOR-280421/407
Out-of-bounds Write	01-04-2021	7.5	An issue was discovered in the reorder crate through 2021-02-24 for Rust. swap_index can return uninitialized values if an iterator returns a len() that is too large. **CVE ID : CVE-2021-29942**	https://rustsec.org/advisories/RUSTSEC-2021-0050.html	A-REO-REOR-280421/408
rocket					
rocket					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-04-2021	7.5	An issue was discovered in the rocket crate before 0.4.7 for Rust. uri::Formatter can have a use-after-free if a user-provided function panics. **CVE ID : CVE-2021-29935**	https://rustsec.org/advisories/RUSTSEC-2021-0044.html	A-ROC-ROCK-280421/409
rocklobster					
contact_form_7					
Cross-Site Request Forgery (CSRF)	05-04-2021	6.8	Due to the lack of sanitization and lack of nonce protection on the custom CSS feature, an attacker could craft a request to inject malicious JavaScript on a site using the Contact Form 7 Style WordPress plugin through 3.1.9. If an attacker successfully tricked a siteâ€™s administrator into clicking a link or attachment, then the request could be sent and the CSS settings would be successfully updated to include malicious JavaScript. **CVE ID : CVE-2021-24159**	https://wpscan.com/vulnerability/363182f1-9fda-4363-8f6a-be37c4c07aa9	A-ROC-CONT-280421/410
rstudio					
shiny_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-04-2021	5	Directory traversal in RStudio Shiny Server before 1.5.16 allows attackers to read the application source code, involving an encoded slash. **CVE ID : CVE-2021-3374**	https://blog.rstudio.com/2021/01/13/shiny-server-1-5-16-update/	A-RST-SHIN-280421/411
rust-lang					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rust					
Double Free	14-04-2021	7.5	In the standard library in Rust before 1.53.0, a double free can occur in the Vec::from_iter function if freeing the element panics. **CVE ID : CVE-2021-31162**	https://github.com/rust-lang/rust/pull/83629	A-RUS-RUST-280421/412
samsung					
account					
Incorrect Default Permissions	09-04-2021	4.6	Using unsafe PendingIntent in Samsung Account in versions 10.8.0.4 in Android P(9.0) and below, and 12.1.1.3 in Android Q(10.0) and above allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent. **CVE ID : CVE-2021-25381**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	A-SAM-ACCO-280421/413
customization_service					
Incorrect Authorization	09-04-2021	4.6	Using unsafe PendingIntent in Customization Service prior to version 2.2.02.1 in Android O(8.x), 2.4.03.0 in Android P(9.0), 2.7.02.1 in Android Q(10.0) and 2.9.01.1 in Android R(11.0) allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent. **CVE ID : CVE-2021-25373**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	A-SAM-CUST-280421/414
experience_service					
Improper Privilege Management	09-04-2021	4.6	Intent redirection in Samsung Experience Service versions 10.8.0.4 in Android P(9.0) below, and	https://security.samsungmobile.com/ser	A-SAM-EXPE-280421/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.0.5 in Android Q(10.0) above allows attacker to execute privileged action. **CVE ID : CVE-2021-25377**	viceWeb.smsb, https://security.samsungmobile.com/	
members					
Incorrect Authorization	09-04-2021	5	An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink in versions 2.4.83.9 in Android O(8.1) and below, and 3.9.00.9 in Android P(9.0) and above allows remote attackers to access a user data related with Samsung Account. **CVE ID : CVE-2021-25374**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	A-SAM-MEMB-280421/416
sap					
commerce					
Improper Control of Generation of Code ('Code Injection')	13-04-2021	6.5	SAP Commerce, versions - 1808, 1811, 1905, 2005, 2011, Backoffice application allows certain authorized users to create source rules which are translated to drools rule when published to certain modules within the application. An attacker with this authorization can inject malicious code in the source rules and perform remote code execution enabling them to compromise the confidentiality, integrity and availability of the application. **CVE ID : CVE-2021-27602**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-COMM-280421/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fiori_apps_2.0_for_travel_management_in_sap_erp					
Missing Authorization	13-04-2021	4	SAP's HCM Travel Management Fiori Apps V2, version - 608, does not perform proper authorization check, allowing an authenticated but unauthorized attacker to read personnel numbers of employees, resulting in escalation of privileges. However, the attacker can only read some information like last name, first name of the employees, so there is some loss of confidential information, Integrity and Availability are not impacted. **CVE ID : CVE-2021-27605**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-FIOR-280421/418
focused_run					
Missing Authorization	13-04-2021	4	SAP Focused RUN versions 200, 300, does not perform necessary authorization checks for an authenticated user, which allows a user to call the oData service and manipulate the activation for the SAP EarlyWatch Alert service data collection and sending to SAP without the intended authorization. **CVE ID : CVE-2021-27609**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-FOCU-280421/419
manufacturing_execution					
Improper Neutralization of Input During Web Page Generation	13-04-2021	3.5	SAP Manufacturing Execution (System Rules), versions - 15.1, 15.2, 15.3, 15.4, allows an authorized attacker to embed malicious code into HTTP	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId	A-SAP-MANU-280421/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			parameter and send it to the server because SAP Manufacturing Execution (System Rules) tab does not sufficiently encode some parameters, resulting in Stored Cross-Site Scripting (XSS) vulnerability. The malicious code can be used for different purposes. e.g., information can be read, modified, and sent to the attacker. However, availability of the server cannot be impacted. **CVE ID : CVE-2021-27600**	=573801649	
netweaver_application_server_java					
Missing Authorization	13-04-2021	5	SAP NetWeaver AS JAVA (Customer Usage Provisioning Servlet), versions - 7.31, 7.40, 7.50, allows an attacker to read some statistical data like product version, traffic, timestamp etc. because of missing authorization check in the servlet. **CVE ID : CVE-2021-27598**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/421
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	3.5	SAP NetWeaver AS Java (Applications based on HTMLB for Java) allows a basic-level authorized attacker to store a malicious file on the server. When a victim tries to open this file, it results in a Cross-Site Scripting (XSS) vulnerability and the attacker can read and modify data. However, the attacker does not have	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control over kind or degree. **CVE ID : CVE-2021-27601**		
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4.3	An unauthorized attacker may be able to entice an administrator to invoke telnet commands of an SAP NetWeaver Application Server for Java that allow the attacker to gain NTLM hashes of a privileged user. **CVE ID : CVE-2021-21485**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/423
Authentication Bypass by Spoofing	13-04-2021	4.3	SAP NetWeaver Application Server Java(HTTP Service), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate logon group in URLs, resulting in a content spoofing vulnerability when directory listing is enabled. **CVE ID : CVE-2021-21492**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/424
netweaver_as_abap					
N/A	13-04-2021	4	An RFC enabled function module SPI_WAIT_MILLIS in SAP NetWeaver AS ABAP, versions - 731, 740, 750, allows to keep a work process busy for any length of time. An attacker could call this function module multiple times to block all work processes thereby causing Denial of Service and affecting the Availability of the SAP system. **CVE ID : CVE-2021-27603**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/425
netweaver_master_data_management					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4.8	SAP NetWeaver Master Data Management, versions - 710, 710.750, allows a malicious unauthorized user with access to the MDM Server subnet to find the password using a brute force method. If successful, the attacker could obtain access to highly sensitive data and MDM administrative privileges leading to information disclosure vulnerability thereby affecting the confidentiality and integrity of the application. This happens when security guidelines and recommendations concerning administrative accounts of an SAP NetWeaver Master Data Management installation have not been thoroughly reviewed. **CVE ID : CVE-2021-21482**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-NETW-280421/426
process_integration					
Exposure of Sensitive Information to an Unauthorized Actor	14-04-2021	4	SAP NetWeaver ABAP Server and ABAP Platform (Process Integration - Integration Builder Framework), versions - 7.10, 7.30, 7.31, 7.40, 7.50, allows an attacker to access information under certain conditions, which would otherwise be restricted. **CVE ID : CVE-2021-27599**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-PROC-280421/427
Improper Restriction of XML External	14-04-2021	4	In order to prevent XML External Entity vulnerability in SAP	https://wiki.scn.sap.com/wiki/	A-SAP-PROC-280421/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			NetWeaver ABAP Server and ABAP Platform (Process Integration - Enterprise Service Repository JAVA Mappings), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, SAP recommends to refer this note. **CVE ID : CVE-2021-27604**	pages/viewpage.action?pageId=573801649	
setup					
Unquoted Search Path or Element	14-04-2021	4.4	An unquoted service path in SAPSetup, version - 9.0, could lead to privilege escalation during the installation process that is performed when an executable file is registered. This could further lead to complete compromise of confidentiality, Integrity and Availability. **CVE ID : CVE-2021-27608**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-SETU-280421/429
solution_manager					
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Under certain conditions SAP Solution Manager, version - 720, allows a high privileged attacker to get access to sensitive information which has a direct serious impact beyond the exploitable component thereby affecting the confidentiality in the application. **CVE ID : CVE-2021-21483**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=573801649	A-SAP-SOLU-280421/430
schneider-electric					
c-bus_toolkit					
Improper Limitation of	13-04-2021	7.5	A CWE-22: Improper Limitation of a Pathname to	https://download.sc	A-SCH-C-BU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when restoring a project. **CVE ID : CVE-2021-22720**	hneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01	280421/431
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2021	6.5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when a file is uploaded. **CVE ID : CVE-2021-22719**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01	A-SCH-C-BU-280421/432
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2021	7.5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when restoring project files. **CVE ID : CVE-2021-22718**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01	A-SCH-C-BU-280421/433
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2021	6.5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when processing config files. **CVE ID : CVE-2021-22717**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01	A-SCH-C-BU-280421/434
Improper	13-04-2021	6.5	A CWE-269: Improper	https://do	A-SCH-C-BU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Privilege Management vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when an unprivileged user modifies a file. **CVE ID : CVE-2021-22716**	wnload.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-103-01	280421/435
seafile					
seafile					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	3.5	Seafile 7.0.5 (2019) allows Persistent XSS via the "share of library functionality." **CVE ID : CVE-2021-30146**	N/A	A-SEA-SEAF-280421/436
sickrage					
sickrage					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	3.5	in SiCKRAGE, versions 4.2.0 to 10.0.11.dev1 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly when processed by the server. Therefore, an attacker can inject arbitrary JavaScript code inside the application, and possibly steal a user's sensitive information. **CVE ID : CVE-2021-25925**	https://github.com/SiCKRAGE/SiCKRAGE/commit/9f42426727e16609ad3d1337f6637588b8ed28e4	A-SIC-SICK-280421/437
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	In SiCKRAGE, versions 9.3.54.dev1 to 10.0.11.dev1 are vulnerable to Reflected Cross-Site-Scripting (XSS) due to user input not being validated properly in the `quicksearch` feature. Therefore, an attacker can	https://github.com/SiCKRAGE/SiCKRAGE/commit/9f42426727e16609ad3d1337	A-SIC-SICK-280421/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			steal a user's sessionID to masquerade as a victim user, to carry out any actions in the context of the user. **CVE ID : CVE-2021-25926**	f6637588b8ed28e4	
slab					
quill					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2021	4.3	A vulnerability in the HTML editor of Slab Quill 4.8.0 allows an attacker to execute arbitrary JavaScript by storing an XSS payload (a crafted onloadstart attribute of an IMG element) in a text field. **CVE ID : CVE-2021-3163**	N/A	A-SLA-QUIL-280421/439
slice-deque_project					
slice-deque					
Double Free	01-04-2021	5	An issue was discovered in the slice-deque crate through 2021-02-19 for Rust. A double drop can occur in SliceDeque::drain_filter upon a panic in a predicate function. **CVE ID : CVE-2021-29938**	https://rustsec.org/advisories/RUSTSEC-2021-0047.html	A-SLI-SLIC-280421/440
softing					
opc_toolbox					
Cross-Site Request Forgery (CSRF)	02-04-2021	6.8	A Cross-Site Request Forgery (CSRF) vulnerability in en/cfg_setpwd.html in Softing AG OPC Toolbox through 4.10.1.13035 allows attackers to reset the administrative password by inducing the Administrator user to	N/A	A-SOF-OPC_-280421/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			browse a URL controlled by an attacker. **CVE ID : CVE-2021-29660**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	3.5	Softing AG OPC Toolbox through 4.10.1.13035 allows /en/diag_values.html Stored XSS via the ITEMLISTVALUES##ITEMID parameter, resulting in JavaScript payload injection into the trace file. This payload will then be triggered every time an authenticated user browses the page containing it. **CVE ID : CVE-2021-29661**	N/A	A-SOF-OPC_-280421/442
solarwinds					
orion_platform					
Improper Access Control	14-04-2021	7.5	This vulnerability allows remote attackers to execute escalate privileges on affected installations of SolarWinds Orion Platform 2020.2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SaveUserSetting endpoint. The issue results from improper restriction of this endpoint to unprivileged users. An attacker can leverage this vulnerability to escalate privileges their privileges from Guest to Administrator. Was ZDI-CAN-11903. **CVE ID : CVE-2021-27258**	N/A	A-SOL-ORIO-280421/443
sonicwall					
email_security					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-04-2021	7.5	A vulnerability in the SonicWall Email Security version 10.0.9.x allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host. **CVE ID : CVE-2021-20021**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007	A-SON-EMAI-280421/444
Unrestricted Upload of File with Dangerous Type	09-04-2021	6.5	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host. **CVE ID : CVE-2021-20022**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0008	A-SON-EMAI-280421/445
global_management_system					
Improper Authentication	10-04-2021	10	A command execution vulnerability in SonicWall GMS 9.3 allows a remote unauthenticated attacker to locally escalate privilege to root. **CVE ID : CVE-2021-20020**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0009	A-SON-GLOB-280421/446
hosted_email_security					
Improper Privilege Management	09-04-2021	7.5	A vulnerability in the SonicWall Email Security version 10.0.9.x allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host. **CVE ID : CVE-2021-20021**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007	A-SON-HOST-280421/447
Unrestricted Upload of File with Dangerous Type	09-04-2021	6.5	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host. **CVE ID : CVE-2021-20022**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-	A-SON-HOST-280421/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0008	
squirro					
squirro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	The Squirro Insights Engine was affected by a Reflected Cross-Site Scripting (XSS) vulnerability affecting versions 2.0.0 up to and including 3.2.4. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes. **CVE ID : CVE-2021-27945**	https://squirro.atlassian.net/wiki/spaces/DOC/pages/2389672672/CVE-2021-27945+-+Cross-Site+Scripting	A-SQU-SQUI-280421/449
stackpath					
ajaxsearchpro					
Deserialization of Untrusted Data	14-04-2021	6.5	AjaxSearchPro before 4.20.8 allows Deserialization of Untrusted Data (in the import database feature of the administration panel), leading to Remote Code execution. **CVE ID : CVE-2021-29654**	N/A	A-STA-AJAX-280421/450
stackvector_project					
stackvector					
Out-of-	01-04-2021	7.5	An issue was discovered in	https://ru	A-STA-STAC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			the stackvector crate through 2021-02-19 for Rust. There is an out-of-bounds write in StackVec::extend if size_hint provides certain anomalous data. **CVE ID : CVE-2021-29939**	stsec.org/advisories/RUSTSEC-2021-0048.html	280421/451
storage_project					
storage					
Improper Locking	01-04-2021	7.1	A deadlock vulnerability was found in 'github.com/containers/storage' in versions before 1.28.1. When a container image is processed, each layer is unpacked using `tar`. If one of those layers is not a valid `tar` archive this causes an error leading to an unexpected situation where the code indefinitely waits for the tar unpacked stream, which never finishes. An attacker could use this vulnerability to craft a malicious image, which when downloaded and stored by an application using containers/storage, would then cause a deadlock leading to a Denial of Service (DoS). **CVE ID : CVE-2021-20291**	https://bugzilla.redhat.com/show_bug.cgi?id=1939485	A-STO-STOR-280421/452
stripe					
stripe					
Improper Neutralization of Special Elements in	01-04-2021	6.8	vscode-stripe is an extension for Visual Studio Code. A vulnerability in Stripe for Visual Studio	https://github.com/stripe/vscode-	A-STR-STRI-280421/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			Code extension exists when it loads an untrusted source-code repository containing malicious settings. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. The update addresses the vulnerability by modifying the way the extension validates its settings. **CVE ID : CVE-2021-21420**	stripe/security/advisories/GHSA-j6x4-4622-8vv3	
suse					
s390-tools					
Insecure Temporary File	14-04-2021	2.1	A Insecure Temporary File vulnerability in s390-tools of SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-SP2 allows local attackers to prevent VM live migrations This issue affects: SUSE Linux Enterprise Server 12-SP5 s390-tools versions prior to 2.1.0-18.29.1. SUSE Linux Enterprise Server 15-SP2 s390-tools versions prior to 2.11.0-9.20.1. **CVE ID : CVE-2021-25316**	https://bugzilla.suse.com/show_bug.cgi?id=1182777	A-SUS-S390-280421/454
svelte					
svelte					
N/A	05-04-2021	6.8	The unofficial Svelte extension before 104.8.0 for Visual Studio Code allows attackers to execute arbitrary code via a crafted workspace configuration. **CVE ID : CVE-2021-29261**	https://github.com/sveltejs/language-tools/commit/5d7bf1fd98bfe2cd208086	A-SVE-SVEL-280421/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				3a3c95ce099b898075	
swiperjs					
swiper					
N/A	12-04-2021	7.5	This affects the package swiper before 6.5.1. **CVE ID : CVE-2021-23370**	https://github.com/nolimits4web/swiper/commit/9dad2739b7474f383474773d5ab898a0c29ac178	A-SWI-SWIP-280421/456
sygnoos					
popup_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	4.3	The "All Subscribers" setting page of Popup Builder was vulnerable to reflected Cross-Site Scripting. **CVE ID : CVE-2021-24152**	https://wpscan.com/vulnerability/597e9686-f4e2-43bf-85ef-c5967e5652bd	A-SYG-POPU-280421/457
syncthing					
syncthing					
Improper Input Validation	06-04-2021	5	Syncthing is a continuous file synchronization program. In Syncthing before version 1.15.0, the relay server `strelaysrv` can be caused to crash and exit by sending a relay message with a negative length field. Similarly, Syncthing itself can crash for the same reason if given a malformed message from a malicious relay server	https://github.com/syncthing/syncthing/commit/fb4fdaf4c0a79c22cad000c42ac1394e3ccb6a97, https://github.com/syncthing/s	A-SYN-SYNC-280421/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when attempting to join the relay. Relay joins are essentially random (from a subset of low latency relays) and Syncthing will by default restart when crashing, at which point it's likely to pick another non-malicious relay. This flaw is fixed in version 1.15.0. **CVE ID : CVE-2021-21404**	yncthing/security/advisories/GHSA-x462-89pf-6r5h	
synology					
diskstation_manager					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-04-2021	9	Improper neutralization of special elements used in an OS command in SYNO.Core.Network.PPPoE in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote authenticated users to execute arbitrary code via realname parameter. **CVE ID : CVE-2021-29083**	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-280421/459
telemetry_project					
telemetry					
N/A	01-04-2021	7.5	An issue was discovered in the telemetry crate through 2021-02-17 for Rust. There is a drop of uninitialized memory if a value.clone() call panics within misc::vec_with_size(). **CVE ID : CVE-2021-29937**	https://rustsec.org/advisories/RUSTSEC-2021-0046.html	A-TEL-TELE-280421/460
tencent					
wechat					
Out-of-bounds Read	14-04-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected	N/A	A-TEN-WECH-280421/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations of Tencent WeChat 2.9.5 desktop version. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the WXAM decoder. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-11907. **CVE ID : CVE-2021-27247**		
teradici					
pcoip_connection_manager_and_security_gateway					
Cleartext Storage of Sensitive Information	06-04-2021	2.1	Sensitive smart card data is logged in default INFO logs by Teradici's PCoIP Connection Manager and Security Gateway prior to version 21.01.3. **CVE ID : CVE-2021-25692**	https://advisory.teradici.com/security-advisories/77/	A-TER-PCOI-280421/462
testimonial_rotator_project					
testimonial_rotator					
Improper Neutralization of Input During Web Page Generation ('Cross-site	05-04-2021	3.5	Stored Cross-Site Scripting vulnerabilities in Testimonial Rotator 3.0.3 allow low privileged users (Contributor) to inject arbitrary JavaScript code or HTML without approval.	https://wpscan.com/vulnerability/8b6f4a77-4008-4730-9a91-	A-TES-TEST-280421/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			This could lead to privilege escalation **CVE ID : CVE-2021-24156**	fa055a8b3e68	
theforeman					
foreman_azurerm					
Exposure of Sensitive Information to an Unauthorized Actor	08-04-2021	6.5	A flaw was found in Red Hat Satellite in tfm-rubygem-foreman_azure_rm in versions before 2.2.0. A credential leak was identified which will expose Azure Resource Manager's secret key through JSON of the API output. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2021-3413**	N/A	A-THE-FORE-280421/464
thekelleys					
dnsmasq					
N/A	08-04-2021	4.3	A flaw was found in dnsmasq in versions before 2.85. When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this	https://bugzilla.redhat.com/show_bug.cgi?id=1939368	A-THE-DNSM-280421/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is to data integrity. **CVE ID : CVE-2021-3448**		
themeeditor					
theme_editor					
Files or Directories Accessible to External Parties	05-04-2021	4	The Theme Editor WordPress plugin before 2.6 did not validate the GET file parameter before passing it to the download_file() function, allowing administrators to download arbitrary files on the web server, such as /etc/passwd **CVE ID : CVE-2021-24154**	https://wpscan.com/vulnerability/566c6836-fc3d-4dd9-b351-c3d9da9ec22e	A-THE-THEM-280421/466
themeisle					
orbit_fox					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	Orbit Fox by ThemeIsle has a feature to add custom scripts to the header and footer of a page or post. There were no checks to verify that a user had the unfiltered_html capability prior to saving the script tags, thus allowing lower-level users to inject scripts that could potentially be malicious. **CVE ID : CVE-2021-24157**	https://wpscan.com/vulnerability/28e42f4e-e38a-4bf4-b51b-d8f21c40f037	A-THE-ORBI-280421/467
Improper Privilege Management	05-04-2021	3.5	Orbit Fox by ThemeIsle has a feature to add a registration form to both the Elementor and Beaver Builder page builders functionality. As part of the registration form, administrators can choose which role to set as the default for users upon	https://wpscan.com/vulnerability/d81d0e72-9bb5-47ef-a796-3b305a4b604f	A-THE-ORBI-280421/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			registration. This field is hidden from view for lower-level users, however, they can still supply the user_role parameter to update the default role for registration. **CVE ID : CVE-2021-24158**		
themeum					
tutor_lms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-04-2021	4	The tutor_mark_answer_as_correct AJAX action from the Tutor LMS â€“ eLearning and online course solution WordPress plugin before 1.7.7 was vulnerable to blind and time based SQL injections that could be exploited by students. **CVE ID : CVE-2021-24181**	https://wpscan.com/vulnerability/d5a00322-7098-4f8d-8e5e-157b63449c17	A-THE-TUTO-280421/469
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-04-2021	4	The tutor_quiz_builder_get_answers_by_question AJAX action from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be exploited by students. **CVE ID : CVE-2021-24182**	https://wpscan.com/vulnerability/f74dfc52-46ba-41e3-994b-23115a22984f	A-THE-TUTO-280421/470
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-04-2021	4	The tutor_quiz_builder_get_question_form AJAX action from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be	https://wpscan.com/vulnerability/9b8da6b7-f1d6-4a7d-a621-4ca01e4b7496	A-THE-TUTO-280421/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by students. **CVE ID : CVE-2021-24183**		
Improper Privilege Management	05-04-2021	6.5	Several AJAX endpoints in the Tutor LMS – eLearning and online course solution WordPress plugin before 1.7.7 were unprotected, allowing students to modify course information and elevate their privileges among many other actions. **CVE ID : CVE-2021-24184**	https://wpscan.com/vulnerability/5e85917c-7a58-49cb-b8b3-05aa18ffff3e	A-THE-TUTO-280421/472
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-04-2021	4	The tutor_place_rating AJAX action from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.7.7 was vulnerable to blind and time based SQL injections that could be exploited by students. **CVE ID : CVE-2021-24185**	https://wpscan.com/vulnerability/0cba5349-e916-43f0-a1fe-62cf73e352a2	A-THE-TUTO-280421/473
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-04-2021	4	The tutor_answering_quiz_question/get_answer_by_id function pair from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be exploited by students. **CVE ID : CVE-2021-24186**	https://wpscan.com/vulnerability/5f5c0c6c-6f76-4366-b590-0aab557f8c60	A-THE-TUTO-280421/474
wp_page_builder					
Incorrect Authorization	05-04-2021	4	By default, the WP Page Builder WordPress plugin before 1.2.4 allows subscriber-level users to edit and make changes to any and all posts pages -	https://wpscan.com/vulnerability/21e7a46f-e9a3-4b20-	A-THE-WP_P-280421/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user roles must be specifically blocked from editing posts and pages. **CVE ID : CVE-2021-24207**	b44a-a5b6ce7b7ce6, https://www.themeum.com/wp-page-builder-updated-v1-2-4/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The editor of the WP Page Builder WordPress plugin before 1.2.4 allows lower-privileged users to insert unfiltered HTML, including JavaScript, into pages via the “Raw HTML” widget and the “Custom HTML” widgets (though the custom HTML widget requires sending a crafted request - it appears that this widget uses some form of client side validation but not server side validation), all of which are added via the “page_builder_data” parameter when performing the “wppb_page_save” AJAX action. It is also possible to insert malicious JavaScript via the “wppb_page_css” parameter (this can be done by closing out the style tag and opening a script tag) when performing the “wppb_page_save” AJAX action. **CVE ID : CVE-2021-24208**	https://wpscan.com/vulnerability/c20e243d-b0de-4ae5-9a0d-b9d02c9b8141, https://www.themeum.com/wp-page-builder-updated-v1-2-4/	A-THE-WP_P-280421/476
thoughtworks					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gocd					
Cross-Site Request Forgery (CSRF)	01-04-2021	9.3	In GoCD, versions 19.6.0 to 21.1.0 are vulnerable to Cross-Site Request Forgery due to missing CSRF protection at the `/go/api/config/backup` endpoint. An attacker can trick a victim to click on a malicious link which could change backup configurations or execute system commands in the post_backup_script field. **CVE ID : CVE-2021-25924**	https://github.com/gocd/gocd/commit/7d0baab0d361c377af84994f95ba76c280048548	A-THO-GOCD-280421/477
through_project					
through					
Double Free	01-04-2021	7.5	An issue was discovered in the through crate through 2021-02-18 for Rust. There is a double free (in through and through_and) upon a panic of the map function. **CVE ID : CVE-2021-29940**	https://rustsec.org/advisories/RUSTSEC-2021-0049.html	A-THR-THRO-280421/478
tibco					
messaging_-_eclipse_mosquitto_distribution_-_bridge					
Incorrect Authorization	14-04-2021	7.2	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-	A-TIB-MESS-280421/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition: versions 1.3.0 and below. **CVE ID : CVE-2021-28826**	2021-tibco-messaging-2021-28826	
messaging_-_eclipse_mosquitto_distribution_-_core					
Incorrect Authorization	14-04-2021	7.2	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-2021-tibco-messaging	A-TIB-MESS-280421/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition: versions 1.3.0 and below. **CVE ID : CVE-2021-28825**	-2021-28825	
timelybills					
timelybills					
Cleartext Storage of Sensitive Information	06-04-2021	4.3	Cleartext Storage in a File or on Disk in TimelyBills <= 1.7.0 for iOS and versions <= 1.21.115 for Android allows attacker who can locally read user's files obtain JWT tokens for user's account due to insufficient cache clearing mechanisms. A threat actor can obtain sensitive user data by decoding the tokens as JWT is signed and encoded, not encrypted. **CVE ID : CVE-2021-26833**	N/A	A-TIM-TIME-280421/481
tms-outsource					
wpdatatables					
Improper	12-04-2021	4	The wpDataTables – Tables	https://w	A-TMS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			& Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'length' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application. **CVE ID : CVE-2021-24200**	pdatatables.com/help/whats-new-changelog/, https://wpscan.com/vulnerability/21aa7e18-0162-45bf-a5c6-ceee64ffa1f9	WPDA-280421/482
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-04-2021	4	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'start' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application. **CVE ID : CVE-2021-24199**	https://wpscan.com/vulnerability/5c98c2d6-d002-4cff-9d6f-633cb3ec6280, https://wpdatatables.com/help/whats-new-changelog/	A-TMS-WPDA-280421/483
Improper Access Control	12-04-2021	5.5	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that	https://wpdatatables.com/help/whats-new-changelog	A-TMS-WPDA-280421/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			visits the page where the table is published can tamper the parameters to delete the data of another user that are present in the same table through id_key and id_val parameters. By exploiting this issue an attacker is able to delete the data of all users in the same table. **CVE ID : CVE-2021-24198**	/, https://wpscan.com/vulnerability/d953bc62-8a6f-445b-a556-bc25cdd200e3	
Improper Access Control	12-04-2021	5.5	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that visits the page where the table is published can tamper the parameters to access the data of another user that are present in the same table by taking over the user permissions on the table through formdata[wdt_ID] parameter. By exploiting this issue an attacker is able to access and manage the data of all users in the same table. **CVE ID : CVE-2021-24197**	https://wpscan.com/vulnerability/a56c04a4-dda0-4a7f-a525-d0349a1fda2b, https://wpdatatables.com/help/whats-new-changelog/	A-TMS-WPDA-280421/485
trendmicro					
apex_one					
Improper Privilege Management	13-04-2021	7.2	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a resource used by the service could allow a	https://success.trendmicro.com/solution/000286157, https://su	A-TRE-APEX-280421/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-25253**	ccess.trendmicro.com/solution/000286019	
Improper Privilege Management	13-04-2021	7.2	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a sensitive file could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-25250**	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-APEX-280421/487
Incorrect Permission Assignment for Critical Resource	13-04-2021	2.1	An insecure file permissions vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to take control of a specific log file on affected installations. **CVE ID : CVE-2021-28646**	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-APEX-280421/488
Incorrect Permission Assignment for Critical	13-04-2021	7.2	An incorrect permission assignment vulnerability in Trend Micro Apex One, Apex One as a Service and	https://success.trendmicro.com/solutio	A-TRE-APEX-280421/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			OfficeScan XG SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-28645**	n/000286157, https://success.trendmicro.com/solution/000286019	
officescan					
Improper Privilege Management	13-04-2021	7.2	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a resource used by the service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-25253**	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-OFFI-280421/490
Improper Privilege Management	13-04-2021	7.2	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a sensitive file could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-OFFI-280421/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in order to exploit this vulnerability. **CVE ID : CVE-2021-25250**		
Incorrect Permission Assignment for Critical Resource	13-04-2021	2.1	An insecure file permissions vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to take control of a specific log file on affected installations. **CVE ID : CVE-2021-28646**	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-OFFI-280421/492
Incorrect Permission Assignment for Critical Resource	13-04-2021	7.2	An incorrect permission assignment vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-28645**	https://success.trendmicro.com/solution/000286157, https://success.trendmicro.com/solution/000286019	A-TRE-OFFI-280421/493
password_manager					
Uncontrolled Search Path Element	13-04-2021	4.4	Trend Micro Password Manager version 5 (Consumer) is vulnerable to a DLL Hijacking vulnerability which could allow an attacker to inject a malicious DLL file during the installation progress and could execute a malicious program each time a user installs a	https://helpcenter.trendmicro.com/en-us/article/TMKA-10282	A-TRE-PASS-280421/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			program. **CVE ID : CVE-2021-28647**		
trestle-auth_project					
trestle-auth					
Cross-Site Request Forgery (CSRF)	13-04-2021	4.3	trestle-auth is an authentication plugin for the Trestle admin framework. A vulnerability in trestle-auth versions 0.4.0 and 0.4.1 allows an attacker to create a form that will bypass Rails' built-in CSRF protection when submitted by a victim with a trestle-auth admin session. This potentially allows an attacker to alter protected data, including admin account credentials. The vulnerability has been fixed in trestle-auth 0.4.2 released to RubyGems. **CVE ID : CVE-2021-29435**	https://github.com/TrestleAdmin/trestle-auth/commit/cb95b05cdb2609052207af07b4b8dfe3a23c11dc, https://github.com/TrestleAdmin/trestle-auth/security/advisories/GHSA-h8hx-2c5r-32cf	A-TRE-TRES-280421/495
tribalsystems					
zenario					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-04-2021	3.5	Cross Site Scripting (XSS) in the "admin_boxes.ajax.php" component of Tribal Systems Zenario CMS v8.8.52729 allows remote attackers to execute arbitrary code by injecting arbitrary HTML into the "cID" parameter when creating a new HTML component. **CVE ID : CVE-2021-27673**	N/A	A-TRI-ZENA-280421/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-04-2021	4	SQL Injection in the "admin_boxes.ajax.php" component of Tribal Systems Zenario CMS v8.8.52729 allows remote attackers to obtain sesnitive database information by injecting SQL commands into the "cID" parameter when creating a new HTML component. **CVE ID : CVE-2021-27672**	N/A	A-TRI-ZENA-280421/497
tsmuxer_project					
tsmuxer					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	4.3	Buffer Overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a malicious WAV file. **CVE ID : CVE-2021-26805**	https://github.com/justdan96/tsMuxer/issues/395	A-TSM-TSMU-280421/498
uclouvain					
openjpeg					
Integer Overflow or Wraparound	14-04-2021	4.3	Integer Overflow in OpenJPEG v2.4.0 allows remote attackers to crash the application, causing a Denial of Service (DoS). This occurs when the attacker uses the command line option "-ImgDir" on a directory that contains 1048576 files. **CVE ID : CVE-2021-29338**	N/A	A-UCL-OPEN-280421/499
uu_od_project					
uu_od					
Out-of-bounds Read	01-04-2021	7.5	An issue was discovered in PartialReader in the uu_od crate before 0.0.4 for Rust.	https://rustsec.org/advisories	A-UU_-UU_O-280421/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Attackers can read the contents of uninitialized memory locations via a user-provided Read operation. **CVE ID : CVE-2021-29934**	/RUSTSEC-2021-0043.html	
valvesoftware					
steam					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-04-2021	6	Valve Steam through 2021-04-10, when a Source engine game is installed, allows remote authenticated users to execute arbitrary code because of a buffer overflow that occurs for a Steam invite after one click. **CVE ID : CVE-2021-30481**	N/A	A-VAL-STEA-280421/501
vestacp					
control_panel					
Improper Link Resolution Before File Access ('Link Following')	08-04-2021	7.2	VestaCP through 0.9.8-24 allows attackers to gain privileges by creating symlinks to files for which they lack permissions. After reading the RKEY value from user.conf under the /usr/local/vesta/data/users/admin directory, the admin password can be changed via a /reset/?action=confirm&user=admin&code= URI. This occurs because chmod is used unsafely. **CVE ID : CVE-2021-30463**	N/A	A-VES-CONT-280421/502
vesta_control_panel					
Improper Privilege	08-04-2021	9	VestaCP through 0.9.8-24 allows the admin user to	N/A	A-VES-VEST-280421/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			escalate privileges to root because the Sudo configuration does not require a password to run /usr/local/vesta/bin scripts. **CVE ID : CVE-2021-30462**		
vigra_computer_vision_library_project					
vigra_computer_vision_library					
Improper Handling of Exceptional Conditions	06-04-2021	4.3	VIGRA Computer Vision Library Version-1-11-1 contains a segmentation fault vulnerability in the impex.hxx read_image_band() function, in which a crafted file can cause a denial of service. **CVE ID : CVE-2021-30046**	N/A	A-VIG-VIGR-280421/504
vim_project					
vim					
N/A	05-04-2021	6.8	VSCodeVim before 1.19.0 allows attackers to execute arbitrary code via a crafted workspace configuration. **CVE ID : CVE-2021-28832**	https://github.com/VSCodeVim/Vim/commit/939df0e7fd55a9840dbd4fb3c907315e2a5ef446	A-VIM-VIM-280421/505
vm_backups_project					
vm_backups					
Cross-Site Request Forgery (CSRF)	05-04-2021	4.3	The VM Backups WordPress plugin through 1.0 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as generate backups of the	https://wpscan.com/vulnerability/187e6967-6961-4843-a9d5-	A-VM_-VM_B-280421/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DB, plugins, and current . **CVE ID : CVE-2021-24172**	866f6ebdb7bc	
Cross-Site Request Forgery (CSRF)	05-04-2021	4.3	The VM Backups WordPress plugin through 1.0 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as update the plugin's options, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24173**	https://wpscan.com/vulnerability/b69ea1bc-3c9b-47d7-a164-c860ee46a9af	A-VM_-VM_B-280421/507
vmware					
carbon_black_cloud_workload					
Improper Authentication	01-04-2021	6.4	VMware Carbon Black Cloud Workload appliance 1.0.0 and 1.01 has an authentication bypass vulnerability that may allow a malicious actor with network access to the administrative interface of the VMware Carbon Black Cloud Workload appliance to obtain a valid authentication token. Successful exploitation of this issue would result in the attacker being able to view and alter administrative configuration settings. **CVE ID : CVE-2021-21982**	https://www.vmware.com/security/advisories/VMSA-2021-0005.html	A-VMW-CARB-280421/508
w1.fi					
hostapd					
Improper Input Validation	02-04-2021	5	In wpa_supplicant and hostapd 2.9, forging attacks may occur because AlgorithmIdentifier parameters are mishandled in tls/pkcs1.c and	https://w1.fi/cgit/hostap/commit/?id=a0541334a6394f823	A-W1.-HOST-280421/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tls/x509v3.c. **CVE ID : CVE-2021-30004**	7a4393b7372693cd7e96f15	
wpa_supplicant					
Improper Input Validation	02-04-2021	5	In wpa_supplicant and hostapd 2.9, forging attacks may occur because AlgorithmIdentifier parameters are mishandled in tls/pkcs1.c and tls/x509v3.c. **CVE ID : CVE-2021-30004**	https://w1.fi/cgit/hostap/commit/?id=a0541334a6394f8237a4393b7372693cd7e96f15	A-W1.-WPA_-280421/510
web-school					
enterprise_resource_planning					
Cross-Site Request Forgery (CSRF)	08-04-2021	4.3	Web-School ERP V 5.0 contains a cross-site request forgery (CSRF) vulnerability that allows a remote attacker to create a voucher payment request through module/accounting/voucher/create. The application fails to validate the CSRF token for a POST request using admin privilege. **CVE ID : CVE-2021-30114**	N/A	A-WEB-ENTE-280421/511
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	4.3	A blind XSS vulnerability exists in Web-School ERP V 5.0 via (Add Events) in event name and description fields. An attacker can inject a JavaScript code that will be stored in the page. If any visitor sees the event, then the payload will be executed and sends the victim's information to the attacker website.	N/A	A-WEB-ENTE-280421/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30113		
Cross-Site Request Forgery (CSRF)	08-04-2021	4.3	Web-School ERP V 5.0 contains a cross-site request forgery (CSRF) vulnerability that allows a remote attacker to create a student_leave_application request through module/core/studentleave application/create. The application fails to validate the CSRF token for a POST request using Guardian privilege. **CVE ID : CVE-2021-30112**	N/A	A-WEB-ENTE-280421/513
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2021	3.5	A stored XSS vulnerability exists in Web-School ERP V 5.0 via (Add Events) in the event name and description fields. An attack can inject a JavaScript code that will be stored in the page. If any visitor sees the events, then the payload will be executed. **CVE ID : CVE-2021-30111**	N/A	A-WEB-ENTE-280421/514
web-stat					
web-stat					
Exposure of Sensitive Information to an Unauthorized Actor	05-04-2021	5	When visiting a site running Web-Stat < 1.4.0, the "wts_web_stat_load_init" function used the visitorâ€™s browser to send an XMLHttpRequest request to https://wts2.one/ajax.htm?action=lookup_WP_account. **CVE ID : CVE-2021-24167**	https://wpscan.com/vulnerability/e7326903-1552-4934-a611-fc0b43236d60	A-WEB-WEB--280421/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webdesi9					
file_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	In the default configuration of the File Manager WordPress plugin before 7.1, a Reflected XSS can occur on the endpoint /wp-admin/admin.php?page=wp_file_manager_properties when a payload is submitted on the User-Agent parameter. The payload is then reflected back on the web application response. **CVE ID : CVE-2021-24177**	https://wpscan.com/vulnerability/1cf3d256-cf4b-4d1f-9ed8-e2cc6392d8d8, https://plugins.trac.wordpress.org/changeset/2476829/	A-WEB-FILE-280421/516
wfiltericf					
wfilter_internet_content_filter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-04-2021	4.3	Wfilter ICF 5.0.117 contains a cross-site scripting (XSS) vulnerability. An attacker in the same LAN can craft a packet with a malicious User-Agent header to inject a payload in its logs, where an attacker can take over the system by through its plugin-running function. **CVE ID : CVE-2021-3243**	N/A	A-WFI-WFIL-280421/517
whatsapp					
whatsapp					
Out-of-bounds Write	06-04-2021	10	A missing bounds check within the audio decoding pipeline for WhatsApp calls in WhatsApp for Android prior to v2.21.3, WhatsApp Business for Android prior to v2.21.3, WhatsApp for iOS prior to v2.21.32, and	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-280421/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WhatsApp Business for iOS prior to v2.21.32 could have allowed an out-of-bounds write. **CVE ID : CVE-2021-24026**		
Exposure of Resource to Wrong Sphere	06-04-2021	5	A cache configuration issue prior to WhatsApp for Android v2.21.4.18 and WhatsApp Business for Android v2.21.4.18 may have allowed a third party with access to the device's external storage to read cached TLS material. **CVE ID : CVE-2021-24027**	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-280421/519
whatsapp_business					
Out-of-bounds Write	06-04-2021	10	A missing bounds check within the audio decoding pipeline for WhatsApp calls in WhatsApp for Android prior to v2.21.3, WhatsApp Business for Android prior to v2.21.3, WhatsApp for iOS prior to v2.21.32, and WhatsApp Business for iOS prior to v2.21.32 could have allowed an out-of-bounds write. **CVE ID : CVE-2021-24026**	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-280421/520
Exposure of Resource to Wrong Sphere	06-04-2021	5	A cache configuration issue prior to WhatsApp for Android v2.21.4.18 and WhatsApp Business for Android v2.21.4.18 may have allowed a third party with access to the device's external storage to read cached TLS material. **CVE ID : CVE-2021-24027**	https://www.whatsapp.com/security/advisories/2021/	A-WHA-WHAT-280421/521
wikimedia					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
parsoid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2021	4.3	An issue was discovered in Wikimedia Parsoid before 0.11.1 and 0.12.x before 0.12.2. An attacker can send crafted wikitext that Utils/WTUtils.php will transform by using a <meta> tag, bypassing sanitization steps, and potentially allowing for XSS. **CVE ID : CVE-2021-30458**	https://www.mediawiki.org/wiki/Parsoid, https://phabricator.wikimedia.org/T279451	A-WIK-PARS-280421/522
williamluis					
wp-curriculo_vitae_free					
Unrestricted Upload of File with Dangerous Type	12-04-2021	7.5	The WP-Curriculo Vitae Free WordPress plugin through 6.3 suffers from an arbitrary file upload issue in page where the [formCadastro] is embed. The form allows unauthenticated user to register and submit files for their profile picture as well as resume, without any file extension restriction, leading to RCE. **CVE ID : CVE-2021-24222**	https://wpscan.com/vulnerability/4d715de6-8595-4da9-808a-04a28e409900	A-WIL-WP-C-280421/523
wire					
wire-webapp					
Exposure of Sensitive Information to an Unauthorized Actor	02-04-2021	4.3	wire-webapp is an open-source front end for Wire, a secure collaboration platform. In wire-webapp before version 2021-03-15-production.0, when being prompted to enter the app-lock passphrase, the typed passphrase will be sent into the most recently used	https://github.com/wireapp/wire-webapp/commit/281f2a9d795f68abe423c116d5da4e1e73a	A-WIR-WIRE-280421/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			chat when the user does not actively give focus to the input field. Input element focus is enforced programatically in version 2021-03-15-production.0. **CVE ID : CVE-2021-21400**	60062, https://github.com/wireapp/wire-webapp/pull/10704, https://github.com/wireapp/wire-webapp/security/advisories/GHSA-cxwr-f2j3-q8hp	
woocommerce					
help_scout					
Unrestricted Upload of File with Dangerous Type	05-04-2021	7.5	The WooCommerce Help Scout WordPress plugin before 2.9.1 (https://woocommerce.com/products/woocommerce-help-scout/) allows unauthenticated users to upload any files to the site which by default will end up in wp-content/uploads/hstmp. **CVE ID : CVE-2021-24212**	https://wpscan.com/vulnerability/cf9305e8-f5bc-45c3-82db-0ef00fd46129	A-WOO-HELP-280421/525
upload_files					
Unrestricted Upload of File with Dangerous Type	05-04-2021	7.5	The WooCommerce Upload Files WordPress plugin before 59.4 ran a single sanitization pass to remove blocked extensions such as .php. It was possible to bypass this and upload a file with a PHP extension by embedding a "blocked" extension within another "blocked" extension in the	https://wpscan.com/vulnerability/ed4288a1-f7e4-455f-b765-5ac343f87194	A-WOO-UPLO-280421/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"wcuf_file_name" parameter. It was also possible to perform a double extension attack and upload files to a different location via path traversal using the "wcuf_current_upload_session_id" parameter. **CVE ID : CVE-2021-24171**		
wphive					
wordpress_related_posts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	The WordPress Related Posts plugin through 3.6.4 contains an authenticated (admin+) stored XSS vulnerability in the title field on the settings page. By exploiting that an attacker will be able to execute JavaScript code in the user's browser. **CVE ID : CVE-2021-24211**	https://wpscan.com/vulnerability/37e0a033-3dee-476d-ae86-68354e8f0b1c	A-WPH-WORD-280421/527
wpruby					
controlled_admin_access					
Improper Access Control	12-04-2021	10	An Improper Access Control vulnerability was discovered in the Controlled Admin Access WordPress plugin before 1.5.2. Uncontrolled access to the website customization functionality and global CMS settings, like /wp-admin/customization.php and /wp-admin/options.php, can lead to a complete compromise of the target resource.	https://wpscan.com/vulnerability/eec0f29f-a985-4285-8eed-d1855d204a20	A-WPR-CONT-280421/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24215		
x2engine					
x2crm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2021	4.3	Cross Site Scripting (XSS) in X2Engine X2CRM v7.1 allows remote attackers to obtain sensitive information by injecting arbitrary web script or HTML via the "Comment" field in "/profile/activity" page. **CVE ID : CVE-2021-27288**	N/A	A-X2E-X2CR-280421/529
yoast					
yoast_seo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-04-2021	3.5	A Stored Cross-Site Scripting vulnerability was discovered in the Yoast SEO WordPress plugin before 3.4.1, which had built-in blacklist filters which were blacklisting Parenthesis as well as several functions such as alert but bypasses were found. **CVE ID : CVE-2021-24153**	https://wpscan.com/vulnerability/77810044-394d-4314-b9a1-20c7dca726dc	A-YOA-YOAS-280421/530
yomi-search_project					
yomi-search					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2021	4.3	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20691**	N/A	A-YOM-YOMI-280421/531
Improper Neutralization of Input	07-04-2021	4.3	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows	N/A	A-YOM-YOMI-280421/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20690**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2021	4.3	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20689**	N/A	A-YOM-YOMI-280421/533
yubico					
yubihsm_connector					
Loop with Unreachable Exit Condition ('Infinite Loop')	14-04-2021	5	An issue was discovered in the /api/connector endpoint handler in Yubico yubihsm-connector before 3.0.1 (in YubiHSM SDK before 2021.04). The handler did not validate the length of the request, which can lead to a state where yubihsm-connector becomes stuck in a loop waiting for the YubiHSM to send it data, preventing any further operations until the yubihsm-connector is restarted. An attacker can send 0, 1, or 2 bytes to trigger this. **CVE ID : CVE-2021-28484**	https://www.yubico.com/support/security-advisories/ysa-2021-02/	A-YUB-YUBI-280421/534
zerof					
expert					
Improper Neutralization of Special Elements used in an	13-04-2021	7.5	The ZEROF Expert pro/2.0 application for mobile devices allows SQL Injection via the Authorization header to the	N/A	A-ZER-EXPE-280421/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			/v2/devices/add endpoint. **CVE ID : CVE-2021-30176**		
web_server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-04-2021	7.5	ZEROF Web Server 1.0 (April 2021) allows SQL Injection via the /HandleEvent endpoint for the login page. **CVE ID : CVE-2021-30175**	N/A	A-ZER-WEB_-280421/536
zeromq					
libzmq					
Uncontrolled Resource Consumption	01-04-2021	4.3	An uncontrolled resource consumption (memory leak) flaw was found in the ZeroMQ client in versions before 4.3.3 in src/pipe.cpp. This issue causes a client that connects to multiple malicious or compromised servers to crash. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-20234**	https://bugzilla.redhat.com/show_bug.cgi?id=1921972, https://github.com/zeromq/libzmq/security/advisories/GHSA-wfr2-29gj-5w87	A-ZER-LIBZ-280421/537
Out-of-bounds Write	01-04-2021	6.8	There's a flaw in the zeromq server in versions before 4.3.3 in src/decoder_allocators.hpp. The decoder static allocator could have its sized changed, but the buffer would remain the same as it is a static buffer. A remote, unauthenticated attacker who sends a crafted request to the	https://bugzilla.redhat.com/show_bug.cgi?id=1921983, https://github.com/zeromq/libzmq/security/advisories/GHSA	A-ZER-LIBZ-280421/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zeromq server could trigger a buffer overflow WRITE of arbitrary data if CURVE/ZAP authentication is not enabled. The greatest impact of this flaw is to application availability, data integrity, and confidentiality. **CVE ID : CVE-2021-20235**	-fc3w-qxf5-7hp6	
zohocorp					
manageengine_opmanager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-04-2021	9.4	Manage Engine OpManager builds below 125346 are vulnerable to a remote denial of service vulnerability due to a path traversal issue in spark gateway component. This allows a remote attacker to remotely delete any directory or directories on the OS. **CVE ID : CVE-2021-20078**	N/A	A-ZOH-MANA-280421/539
manageengine_servicedesk_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2021	4.3	Insufficient output sanitization in ManageEngine ServiceDesk Plus before version 11200 and ManageEngine AssetExplorer before version 6800 allows a remote, unauthenticated attacker to conduct persistent cross-site scripting (XSS) attacks by uploading a crafted XML asset file. **CVE ID : CVE-2021-20080**	N/A	A-ZOH-MANA-280421/540
zulip					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
zulip_server					
Incorrect Permission Assignment for Critical Resource	15-04-2021	4	In the topic moving API in Zulip Server 3.x before 3.4, organization administrators were able to move messages to streams in other organizations hosted by the same Zulip installation. **CVE ID : CVE-2021-30487**	https://blog.zulip.com/2021/04/14/zulip-server-3-4/	A-ZUL-ZULI-280421/541
Incorrect Permission Assignment for Critical Resource	15-04-2021	5	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of the all_public_streams API feature resulted in guest users being able to receive message traffic to public streams that should have been only accessible to members of the organization. **CVE ID : CVE-2021-30479**	https://blog.zulip.com/2021/04/14/zulip-server-3-4/	A-ZUL-ZULI-280421/542
Incorrect Permission Assignment for Critical Resource	15-04-2021	4	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of the can_forge_sender permission (previously is_api_super_user) resulted in users with this permission being able to send messages appearing as if sent by a system bot, including to other organizations hosted by the same Zulip installation. **CVE ID : CVE-2021-30478**	https://blog.zulip.com/2021/04/14/zulip-server-3-4/	A-ZUL-ZULI-280421/543
Incorrect Permission Assignment for Critical Resource	15-04-2021	4	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of replies to messages sent by outgoing webhooks to private streams meant that	https://blog.zulip.com/2021/04/14/zulip-server-	A-ZUL-ZULI-280421/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an outgoing webhook bot could be used to send messages to private streams that the user was not intended to be able to send messages to. **CVE ID : CVE-2021-30477**	3-4/	
Hardware					
asus					
asmb8-ikvm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	https://www.twcert.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/545
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-ASMB-280421/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28176	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	H-ASU-ASMB-280421/547
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The UEFI configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	https://www.twcert.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-ASMB-280421/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28179**	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/549
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/550
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video configuration	https://www.twcert.org.tw/tw/cp-132-	H-ASU-ASMB-280421/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28182**	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	H-ASU-ASMB-280421/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4554-10a74-1.html	H-ASU-ASMB-280421/554
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28185**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-ASMB-280421/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4555-3c7c3-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	H-ASU-ASMB-280421/556
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28188**	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/559
Improper Neutralization of Special Elements used in an OS	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4573-	H-ASU-ASMB-280421/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28204**	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/561
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.com/conte	H-ASU-ASMB-280421/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access system files. **CVE ID : CVE-2021-28205**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
asmb9-ikvm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/563
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-ASMB-280421/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-ASMB-280421/565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/567
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/568
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify	https://www.asus.com/content/ASUS-Product-	H-ASU-ASMB-280421/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/conte	H-ASU-ASMB-280421/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-ASMB-280421/572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-ASMB-280421/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/574
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ASMB-280421/575
Improper	06-04-2021	6.8	The specific function in	https://w	H-ASU-ASMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	ww.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/576
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-ASMB-280421/577
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-	H-ASU-ASMB-280421/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-ASMB-280421/579
e700_g4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/conte	H-ASU-E700-280421/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-E700-280421/581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-E700-280421/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/584
Buffer Copy	06-04-2021	4	The Radius configuration	https://w	H-ASU-E700-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	ww.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-E700-280421/586
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4567-34350-	H-ASU-E700-280421/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/588
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-E700-280421/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	us/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-E700-280421/590
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	H-ASU-E700-280421/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/592
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/593
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.asus.c	H-ASU-E700-280421/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-E700-280421/595
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-E700-280421/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
esc4000_dhd_g4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/597
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-ESC4-280421/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28191**	us/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-ESC4-280421/599
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-ESC4-280421/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/602
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.asus.c	H-ASU-ESC4-280421/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html,	H-ASU-ESC4-280421/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-ESC4-280421/606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	H-ASU-ESC4-280421/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28200	https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/608
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/su	H-ASU-ESC4-280421/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/610
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-ESC4-280421/611
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get	https://www.twcert.org.tw/tw	H-ASU-ESC4-280421/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-ESC4-280421/613
esc4000_g4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html,	H-ASU-ESC4-280421/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-ESC4-280421/615
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	H-ASU-ESC4-280421/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Web service. **CVE ID : CVE-2021-28192**	https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-ESC4-280421/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/619
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-ESC4-280421/620
Buffer Copy without Checking Size	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-ESC4-280421/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/622
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-ESC4-280421/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-ESC4-280421/624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	H-ASU-ESC4-280421/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/626
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-ESC4-280421/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-ESC4-280421/628
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/629
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does	https://www.asus.com/content/ASUS-	H-ASU-ESC4-280421/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
esc4000_g4x					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-ESC4-280421/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-ESC4-280421/633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-ESC4-280421/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-ESC4-280421/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-ESC4-280421/637
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/638
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not	https://www.twcert.org.tw/tw/cp-132-	H-ASU-ESC4-280421/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-ESC4-280421/640
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-ESC4-280421/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/642
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html,	H-ASU-ESC4-280421/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/644
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-ESC4-280421/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC4-280421/646
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-ESC4-280421/647
esc8000_g4					
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate	https://www.twcert.org.tw/tw/cp-132-	H-ASU-ESC8-280421/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-ESC8-280421/649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-ESC8-280421/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/651
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-ESC8-280421/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/653
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-ESC8-280421/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/655
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/656
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify	https://www.asus.com/content/ASUS-Product-	H-ASU-ESC8-280421/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-ESC8-280421/658
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	H-ASU-ESC8-280421/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/660
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-ESC8-280421/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-ESC8-280421/662
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/663
Improper	06-04-2021	6.8	The specific function in	https://w	H-ASU-ESC8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	280421/664
esc8000_g4/10g					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/665
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	H-ASU-ESC8-280421/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-ESC8-280421/667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/conte	H-ASU-ESC8-280421/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/669
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-ESC8-280421/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-ESC8-280421/671
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/672
Buffer Copy	06-04-2021	4	The Firmware protocol	https://w	H-ASU-ESC8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	ww.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-ESC8-280421/674
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-ESC8-280421/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/676
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-ESC8-280421/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28202**	4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/678
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-ESC8-280421/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-ESC8-280421/680
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-ESC8-280421/681
knpa-u16					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/682
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-KNPA-280421/683
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	H-ASU-KNPA-280421/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	H-ASU-KNPA-280421/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/687
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-KNPA-280421/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/690
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-KNPA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-KNPA-280421/692
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-KNPA-280421/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-KNPA-280421/694
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	H-ASU-KNPA-280421/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-KNPA-280421/696
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-KNPA-280421/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-KNPA-280421/698
pro_e800_g4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-PRO_-280421/700
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-PRO_-280421/701
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	H-ASU-PRO_-280421/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	H-ASU-PRO_-280421/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-PRO_-280421/705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-PRO_-280421/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/707
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-PRO_-280421/708
Buffer Copy	06-04-2021	4	The CD media	https://w	H-ASU-PRO_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/709
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/710
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-PRO_-280421/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/712
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-PRO_-280421/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-PRO_-280421/714
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-PRO_-280421/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
rs100-e10-pi2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS10-280421/716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS10-280421/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS10-280421/718
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS10-280421/719
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	H-ASU-RS10-280421/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS10-280421/721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS10-280421/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS10-280421/723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS10-280421/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS10-280421/725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS10-280421/726
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	H-ASU-RS10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS10-280421/728
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	H-ASU-RS10-280421/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS10-280421/730
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS10-280421/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS10-280421/732
rs300-e10-ps4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS30-280421/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS30-280421/734
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS30-280421/735
Buffer Copy	06-04-2021	4	The SMTP configuration	https://w	H-ASU-RS30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	ww.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/736
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/737
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4565-59c97-	H-ASU-RS30-280421/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS30-280421/739
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS30-280421/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28197**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/741
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS30-280421/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS30-280421/743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/744
Buffer Copy without	06-04-2021	4	The Service configuration-2 function in ASUS BMC's	https://www.asus.c	H-ASU-RS30-280421/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/746
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS30-280421/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/748
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	H-ASU-RS30-280421/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs300-e10-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS30-280421/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS30-280421/752
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/753
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.twcert	H-ASU-RS30-280421/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/755
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS30-280421/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/757
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS30-280421/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28198	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS30-280421/759
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-	H-ASU-RS30-280421/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS30-280421/762
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record	https://www.twcert.org.tw/tw	H-ASU-RS30-280421/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS30-280421/764
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://w	H-ASU-RS30-280421/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS30-280421/766
rs500-e9-ps4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS50-280421/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28190**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS50-280421/768
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-	H-ASU-RS50-280421/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/771
Buffer Copy without Checking Size	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-RS50-280421/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS50-280421/773
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://w	H-ASU-RS50-280421/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	H-ASU-RS50-280421/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28199	ww.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS50-280421/777
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/call	H-ASU-RS50-280421/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/779
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/780
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not	https://www.asus.com/content/ASUS-	H-ASU-RS50-280421/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/782
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS50-280421/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28209**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs500-e9-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	H-ASU-RS50-280421/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28191	ww.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS50-280421/786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS50-280421/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/788
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/789
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate	https://www.asus.com/content/ASUS-	H-ASU-RS50-280421/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/791
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.c	H-ASU-RS50-280421/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS50-280421/793
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-RS50-280421/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/795
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/797
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS50-280421/798
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4578-	H-ASU-RS50-280421/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS50-280421/800
rs500-e9-rs4-u					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.c	H-ASU-RS50-280421/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS50-280421/802
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-RS50-280421/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS50-280421/807
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4567-	H-ASU-RS50-280421/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/809
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS50-280421/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS50-280421/811
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://w	H-ASU-RS50-280421/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/813
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/814
Improper	06-04-2021	6.8	The specific function in	https://w	H-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	280421/815
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/816
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS50-280421/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs500a-e10-ps4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/818
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS50-280421/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS50-280421/820
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS50-280421/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/822
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/823
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	280421/824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/825
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4568-627f7-	H-ASU-RS50-280421/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS50-280421/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS50-280421/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28200**	us/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/829
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	H-ASU-RS50-280421/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/831
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS50-280421/832
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	H-ASU-RS50-280421/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS50-280421/834
rs500a-e10-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-	H-ASU-RS50-280421/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS50-280421/836
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS50-280421/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	us/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/838
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS50-280421/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/840
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS50-280421/841
Buffer Copy without	06-04-2021	4	The Active Directory configuration function in	https://www.twcert	H-ASU-RS50-280421/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS50-280421/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS50-280421/845
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-	H-ASU-RS50-280421/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28201	d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/847
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS50-280421/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS50-280421/849
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/850
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete	https://www.asus.com/conte	H-ASU-RS50-280421/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs500a-e9_rs4_u					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/852
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS50-280421/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS50-280421/854
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS50-280421/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28193	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS50-280421/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS50-280421/858
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/859
Buffer Copy without Checking Size	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-RS50-280421/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS50-280421/861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS50-280421/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/863
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	H-ASU-RS50-280421/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/865
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-	H-ASU-RS50-280421/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/867
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS50-280421/868
rs500a-e9-ps4					
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.twcert.org.tw/tw	H-ASU-RS50-280421/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS50-280421/870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS50-280421/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/872
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS50-280421/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28194	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/874
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-	H-ASU-RS50-280421/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/876
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/877
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information	https://www.asus.com/content/ASUS-	H-ASU-RS50-280421/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS50-280421/879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	H-ASU-RS50-280421/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/881
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS50-280421/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS50-280421/883
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS50-280421/885
rs500a-e9-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/886
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	H-ASU-RS50-280421/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS50-280421/888
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.c	H-ASU-RS50-280421/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/890
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS50-280421/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS50-280421/892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/894
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS50-280421/895
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	H-ASU-RS50-280421/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	H-ASU-RS50-280421/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/899
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-RS50-280421/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS50-280421/901
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS50-280421/902
rs520-e9-rs12-e					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS52-280421/904
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	H-ASU-RS52-280421/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	H-ASU-RS52-280421/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/908
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-RS52-280421/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/911
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-RS52-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS52-280421/913
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS52-280421/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/915
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS52-280421/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS52-280421/917
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS52-280421/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS52-280421/919
rs520-e9-rs8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS52-280421/921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS52-280421/922
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	H-ASU-RS52-280421/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	H-ASU-RS52-280421/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS52-280421/926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS52-280421/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS52-280421/929
Buffer Copy	06-04-2021	4	The CD media	https://w	H-ASU-RS52-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/930
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/931
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS52-280421/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/933
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS52-280421/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS52-280421/935
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS52-280421/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
rs700-e9-rs12					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS70-280421/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS70-280421/939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/940
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	H-ASU-RS70-280421/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS70-280421/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS70-280421/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS70-280421/946
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS70-280421/947
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	H-ASU-RS70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/949
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	H-ASU-RS70-280421/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS70-280421/951
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS70-280421/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS70-280421/953
rs700-e9-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS70-280421/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS70-280421/955
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS70-280421/956
Buffer Copy	06-04-2021	4	The SMTP configuration	https://w	H-ASU-RS70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	ww.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/958
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4565-59c97-	H-ASU-RS70-280421/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS70-280421/960
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS70-280421/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28197**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/962
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS70-280421/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS70-280421/964
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/965
Buffer Copy without	06-04-2021	4	The Service configuration-2 function in ASUS BMC's	https://www.asus.c	H-ASU-RS70-280421/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/967
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS70-280421/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/969
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	H-ASU-RS70-280421/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs700a-e9-rs12v2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/971
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS70-280421/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS70-280421/973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/974
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.twcert	H-ASU-RS70-280421/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/976
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS70-280421/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/978
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS70-280421/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28198	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS70-280421/980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-	H-ASU-RS70-280421/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/982
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/983
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record	https://www.twcert.org.tw/tw	H-ASU-RS70-280421/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS70-280421/985
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://w	H-ASU-RS70-280421/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS70-280421/987
rs700a-e9-rs4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS70-280421/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28190**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS70-280421/989
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-	H-ASU-RS70-280421/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/992
Buffer Copy without Checking Size	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-RS70-280421/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS70-280421/994
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://w	H-ASU-RS70-280421/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	H-ASU-RS70-280421/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28199	ww.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS70-280421/998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/call	H-ASU-RS70-280421/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1000
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1001
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not	https://www.asus.com/content/ASUS-	H-ASU-RS70-280421/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1003
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS70-280421/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28209**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs700a-e9-rs4v2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1005
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	H-ASU-RS70-280421/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28191	ww.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS70-280421/1007
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS70-280421/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1009
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1010
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate	https://www.asus.com/content/ASUS-	H-ASU-RS70-280421/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1012
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.c	H-ASU-RS70-280421/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS70-280421/1014
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-RS70-280421/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS70-280421/1018
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS70-280421/1019
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4578-	H-ASU-RS70-280421/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS70-280421/1021
rs720-e9-rs12-e					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.c	H-ASU-RS72-280421/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-RS72-280421/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1025
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS72-280421/1028
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4567-	H-ASU-RS72-280421/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1030
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS72-280421/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS72-280421/1032
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://w	H-ASU-RS72-280421/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1034
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1035
Improper	06-04-2021	6.8	The specific function in	https://w	H-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	280421/1036
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1037
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS72-280421/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs720-e9-rs24-u					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1039
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS72-280421/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS72-280421/1041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS72-280421/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1044
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	280421/1045
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1046
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4568-627f7-	H-ASU-RS72-280421/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS72-280421/1048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS72-280421/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28200**	us/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1050
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	H-ASU-RS72-280421/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1052
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS72-280421/1053
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	H-ASU-RS72-280421/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1055
rs720-e9-rs8-g					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-	H-ASU-RS72-280421/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS72-280421/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	us/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1059
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS72-280421/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS72-280421/1062
Buffer Copy without	06-04-2021	4	The Active Directory configuration function in	https://www.twcert	H-ASU-RS72-280421/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS72-280421/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS72-280421/1066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-	H-ASU-RS72-280421/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28201	d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1068
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS72-280421/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS72-280421/1070
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1071
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete	https://www.asus.com/conte	H-ASU-RS72-280421/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs720a-e9-rs12v2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1073
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS72-280421/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS72-280421/1075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-RS72-280421/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28193	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1077
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS72-280421/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS72-280421/1079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1080
Buffer Copy without Checking Size	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-RS72-280421/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS72-280421/1082
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS72-280421/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	H-ASU-RS72-280421/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1086
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-	H-ASU-RS72-280421/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1088
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1089
rs720a-e9-rs24-e					
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.twcert.org.tw/tw	H-ASU-RS72-280421/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1091
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS72-280421/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1093
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS72-280421/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28194	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-	H-ASU-RS72-280421/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1098
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information	https://www.asus.com/content/ASUS-	H-ASU-RS72-280421/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS72-280421/1100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	H-ASU-RS72-280421/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1102
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS72-280421/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS72-280421/1104
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1106
rs720a-e9-rs24v2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1107
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	H-ASU-RS72-280421/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS72-280421/1109
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.c	H-ASU-RS72-280421/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1111
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-RS72-280421/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS72-280421/1113
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS72-280421/1116
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	H-ASU-RS72-280421/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1118
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	H-ASU-RS72-280421/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1120
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-RS72-280421/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1122
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1123
rs720q-e9-rs24-s					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1124
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1125
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	H-ASU-RS72-280421/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1127
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	H-ASU-RS72-280421/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-RS72-280421/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1132
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/1133
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS72-280421/1134
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS72-280421/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1136
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS72-280421/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS72-280421/1138
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-RS72-280421/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1140
rs720q-e9-rs8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS72-280421/1143
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	H-ASU-RS72-280421/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	H-ASU-RS72-280421/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-RS72-280421/1147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS72-280421/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS72-280421/1150
Buffer Copy	06-04-2021	4	The CD media	https://w	H-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/1151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1152
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-RS72-280421/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1154
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-RS72-280421/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1156
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-RS72-280421/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
rs720q-e9-rs8-s					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1158
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-RS72-280421/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-RS72-280421/1160
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1161
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	H-ASU-RS72-280421/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1163
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-RS72-280421/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-RS72-280421/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-RS72-280421/1167
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-RS72-280421/1168
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	H-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/1169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-RS72-280421/1170
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	H-ASU-RS72-280421/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-RS72-280421/1172
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	H-ASU-RS72-280421/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-RS72-280421/1174
rt-ac1750_b1					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-	H-ASU-RT-A-280421/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac1900					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1176
rt-ac1900p					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware <	https://www.asus.com/supportonly/RT-	H-ASU-RT-A-280421/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac1900u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.c	H-ASU-RT-A-280421/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac2900					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1179
rt-ac3100					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.c	H-ASU-RT-A-280421/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac5300					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download	H-ASU-RT-A-280421/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/	
rt-ac58u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1182
rt-ac65u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-	H-ASU-RT-A-280421/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac66u_b1					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1184
rt-ac68p					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS	https://www.asus.com/suppo	H-ASU-RT-A-280421/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	rtonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac68r					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://w	H-ASU-RT-A-280421/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	ww.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac68rw					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1187
rt-ac68u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://w	H-ASU-RT-A-280421/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	ww.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac68w					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_	H-ASU-RT-A-280421/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				download /	
rt-ac85u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1190
rt-ac86u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/W	H-ASU-RT-A-280421/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	iFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac88u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1192
rt-ax3000					
Excessive	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-	https://www.asus.c	H-ASU-RT-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Iteration			AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	280421/1193
rt-ax55					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/,	H-ASU-RT-A-280421/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax56u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1195
rt-ax58u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/,	H-ASU-RT-A-280421/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax68u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/	H-ASU-RT-A-280421/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				HelpDesk_download/	
rt-ax82u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1198
rt-ax86u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-	H-ASU-RT-A-280421/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax88u					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-RT-A-280421/1200
ws_c422_pro/se					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1201
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-WS_C-280421/1202
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	H-ASU-WS_C-280421/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1204
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	H-ASU-WS_C-280421/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-WS_C-280421/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1208
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1209
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-WS_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/1210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-WS_C-280421/1211
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-WS_C-280421/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1213
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	H-ASU-WS_C-280421/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-WS_C-280421/1215
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-WS_C-280421/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-WS_C-280421/1217
ws_c621e_sage					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-WS_C-280421/1219
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-WS_C-280421/1220
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	H-ASU-WS_C-280421/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1222
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	H-ASU-WS_C-280421/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-WS_C-280421/1224
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-WS_C-280421/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1226
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-WS_C-280421/1227
Buffer Copy	06-04-2021	4	The CD media	https://w	H-ASU-WS_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/1228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1229
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-WS_C-280421/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1231
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-WS_C-280421/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_C-280421/1233
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-WS_C-280421/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
ws_x299_pro/se					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_X-280421/1235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-WS_X-280421/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-WS_X-280421/1237
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_X-280421/1238
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	H-ASU-WS_X-280421/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_X-280421/1240
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-WS_X-280421/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-WS_X-280421/1242
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-WS_X-280421/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-WS_X-280421/1244
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-WS_X-280421/1245
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	H-ASU-WS_X-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/1246
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-WS_X-280421/1247
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	H-ASU-WS_X-280421/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-WS_X-280421/1249
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	H-ASU-WS_X-280421/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-WS_X-280421/1251
z10pe-d16_ws					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	https://www.twcert.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-Z10P-280421/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28176**	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1253
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	H-ASU-Z10P-280421/1254
Buffer Copy	06-04-2021	4	The UEFI configuration	https://w	H-ASU-Z10P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	ww.twcert.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/1255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28179**	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1256
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users,	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-	H-ASU-Z10P-280421/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	https://www.twcert.org.tw/tw/cp-132-4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1258
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-	H-ASU-Z10P-280421/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28182**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1260
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-Z10P-280421/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4554-10a74-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28185**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4555-3c7c3-1.html	H-ASU-Z10P-280421/1262
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	H-ASU-Z10P-280421/1263
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.asus.c	H-ASU-Z10P-280421/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28188**	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1265
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html,	H-ASU-Z10P-280421/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	https://www.twcert.org.tw/tw/cp-132-4573-aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1267
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary.	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-Z10P-280421/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28204	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28205**	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1269
z10pr-d16					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	https://www.twcert.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-Z10P-280421/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28176**	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1271
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	H-ASU-Z10P-280421/1272
Buffer Copy without	06-04-2021	4	The UEFI configuration function in ASUS BMC's	https://www.twcert	H-ASU-Z10P-280421/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28179**	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users, resulting in a Buffer	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-1.html,	H-ASU-Z10P-280421/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	https://www.twcert.org.tw/tw/cp-132-4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-Product-	H-ASU-Z10P-280421/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28182	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4554-	H-ASU-Z10P-280421/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				10a74-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28185**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4555-3c7c3-1.html	H-ASU-Z10P-280421/1280
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	H-ASU-Z10P-280421/1281
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.asus.com/conte	H-ASU-Z10P-280421/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	nt/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28188**	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1283
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html, https://w	H-ASU-Z10P-280421/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	https://www.twcert.org.tw/tw/cp-132-4573-aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1285
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28204**	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-Z10P-280421/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28205**	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z10P-280421/1287
z11pa-d8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	H-ASU-Z11P-280421/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-Z11P-280421/1289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-Z11P-280421/1290
Buffer Copy without Checking Size	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	H-ASU-Z11P-280421/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1292
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://w	H-ASU-Z11P-280421/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-Z11P-280421/1294
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-	H-ASU-Z11P-280421/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1296
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-	H-ASU-Z11P-280421/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-Z11P-280421/1298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1299
Buffer Copy without Checking Size of Input	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	H-ASU-Z11P-280421/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1301
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-Z11P-280421/1302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28207**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1303
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	H-ASU-Z11P-280421/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4579-c8827-1.html	
z11pa-d8c					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1305
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-	H-ASU-Z11P-280421/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-Z11P-280421/1307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1308
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration	https://www.twcert.org.tw/tw/cp-132-	H-ASU-Z11P-280421/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1310
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	H-ASU-Z11P-280421/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1312
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-Z11P-280421/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-Z11P-280421/1314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-Z11P-280421/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1316
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1317
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4576-	H-ASU-Z11P-280421/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-Z11P-280421/1319
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/conte	H-ASU-Z11P-280421/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access system files. **CVE ID : CVE-2021-28208**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-Z11P-280421/1321
z11pa-u12					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	H-ASU-Z11P-280421/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28190	https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-Z11P-280421/1323
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-Z11P-280421/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1326
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4565-	H-ASU-Z11P-280421/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-Z11P-280421/1328
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/conte	H-ASU-Z11P-280421/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1330
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-Z11P-280421/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-Z11P-280421/1332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1333
Buffer Copy	06-04-2021	4	The Service configuration-2	https://w	H-ASU-Z11P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/1334
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1335
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-Z11P-280421/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1337
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	H-ASU-Z11P-280421/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28209	us/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
z11pa-u12/10g-2s					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	H-ASU-Z11P-280421/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	H-ASU-Z11P-280421/1341
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1342
Buffer Copy	06-04-2021	4	The specific function in	https://w	H-ASU-Z11P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	ww.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/1343
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1344
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered	https://www.asus.com/content/ASUS-Product-Security-	H-ASU-Z11P-280421/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1346
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-	H-ASU-Z11P-280421/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28198**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	H-ASU-Z11P-280421/1348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-Z11P-280421/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1351
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	H-ASU-Z11P-280421/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	H-ASU-Z11P-280421/1353
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html,	H-ASU-Z11P-280421/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	H-ASU-Z11P-280421/1355
z11pr-d16					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-	H-ASU-Z11P-280421/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	H-ASU-Z11P-280421/1357
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	H-ASU-Z11P-280421/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1359
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1360
Buffer Copy without	06-04-2021	4	The Radius configuration function in ASUS BMC's	https://www.twcert	H-ASU-Z11P-280421/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	H-ASU-Z11P-280421/1362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html,	H-ASU-Z11P-280421/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	H-ASU-Z11P-280421/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	H-ASU-Z11P-280421/1366
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/su	H-ASU-Z11P-280421/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1368
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1369
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get	https://www.asus.com/conte	H-ASU-Z11P-280421/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	H-ASU-Z11P-280421/1371
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	H-ASU-Z11P-280421/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
zenwifi_ax_(xt8)					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	H-ASU-ZENW-280421/1373
cisco					
rv110w					
Improper Restriction of	08-04-2021	10	A vulnerability in the web-based management	https://tools.cisco.c	H-CIS-RV11-280421/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	
rv130					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	H-CIS-RV13-280421/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**		
rv130w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	H-CIS-RV13-280421/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1459		
rv132w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV13-280421/1377
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV13-280421/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV13-280421/1379
rv134w					
Improper Restriction of Operations within the	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco	https://tools.cisco.com/security/center/	H-CIS-RV13-280421/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV13-280421/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV13-280421/1382
rv160					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-	H-CIS-RV16-280421/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV16-280421/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV16-280421/1385
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV16-280421/1386
rv160w					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV16-280421/1387
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV16-280421/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV16-280421/1389
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-RV16-280421/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	sb-rv-bypass-inject-Rbhgvfdx	
rv215w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	H-CIS-RV21-280421/1391
rv260					
Improper Restriction of Operations within the	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco	https://tools.cisco.com/security/center/	H-CIS-RV26-280421/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1394
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-	H-CIS-RV26-280421/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Details section of this advisory. **CVE ID : CVE-2021-1472**	Rbhgvfdx	
rv260p					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1396
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1398
Improper Restriction of Operations	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of	https://tools.cisco.com/securi	H-CIS-RV26-280421/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	
rv260w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1400
Improper Restriction of Operations	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP)	https://tools.cisco.com/securi	H-CIS-RV26-280421/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV26-280421/1402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV26-280421/1403
rv340					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1405
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory	H-CIS-RV34-280421/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**	/cisco-sa-sb-rv34x-rce-8bfG2h6b	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1408
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1410
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1473		
rv340w					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1412
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1415
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1417
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-RV34-280421/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	sb-rv-bypass-inject-Rbhgvfdx	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1419
rv345					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1421
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-RV34-280421/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**	yAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1424
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1426
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-1473**		
rv345p					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1428
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	H-CIS-RV34-280421/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on the device. **CVE ID : CVE-2021-1413**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1431
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	H-CIS-RV34-280421/1433
Improper Restriction of Operations within the Bounds of a Memory	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-RV34-280421/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	yAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	H-CIS-RV34-280421/1435
d-link					
dsl-320b-d1					
Out-of-bounds Write	07-04-2021	10	** UNSUPPORTED WHEN ASSIGNED ** D-Link DSL-320B-D1 devices through EU_1.25 are prone to multiple Stack-Based Buffer Overflows that allow unauthenticated remote attackers to take over a device via the login.xgi user and pass parameters. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-26709**	https://www.dlink.com/en/security-bulletin, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10216	H-D-L-DSL--280421/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dlink					
dir-802					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-04-2021	5.8	** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered on D-Link DIR-802 A1 devices through 1.00b05. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-29379**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10206	H-DLI-DIR--280421/1437
dir-816					
Out-of-bounds Write	14-04-2021	7.5	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. Within the handler function of the /goform/addassignment route, a very long text entry for the"'s_ip" and "s_mac" fields could lead to a Stack-Based Buffer Overflow and overwrite the return address. **CVE ID : CVE-2021-27114**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--280421/1438
Improper Neutralization of Special Elements used in an OS Command ('OS Command	14-04-2021	10	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. An HTTP request parameter is used in command string construction within the handler function of the /goform/addRouting route. This could lead to	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--280421/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			Command Injection via Shell Metacharacters. **CVE ID : CVE-2021-27113**		
dir-878					
Out-of-bounds Write	02-04-2021	7.5	An issue was discovered in prog.cgi on D-Link DIR-878 1.30B08 devices. Because strcat is misused, there is a stack-based buffer overflow that does not require authentication. **CVE ID : CVE-2021-30072**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10217	H-DLI-DIR--280421/1440
fireeye					
ex_3500					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-04-2021	4	eMPS 9.0.1.923211 on FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the sort_by parameter to the email search feature. According to the vendor, the issue is fixed in 9.0.3. NOTE: this is different from CVE-2020-25034 and affects newer versions of the software. **CVE ID : CVE-2021-28969**	N/A	H-FIR-EX_3-280421/1441
Improper Neutralization of Special Elements used in an SQL	01-04-2021	4	eMPS 9.0.1.923211 on the Central Management of FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection	N/A	H-FIR-EX_3-280421/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			attacks via the job_id parameter to the email search feature. According to the vendor, the issue is fixed in 9.0.3. **CVE ID : CVE-2021-28970**		
genexis					
platinum_4410					
N/A	13-04-2021	7.5	Genexis PLATINUM 4410 2.1 P4410-V2-1.28 devices allow remote attackers to execute arbitrary code via shell metacharacters to sys_config_valid.xgi, as demonstrated by the sys_config_valid.xgi?exeshell=%60telnetd%20%26%60 URI. **CVE ID : CVE-2021-29003**	N/A	H-GEN-PLAT-280421/1443
hpe					
superdome_flex_server					
N/A	01-04-2021	4	A potential security vulnerability has been identified in HPE Superdome Flex server. A denial of service attack can be remotely exploited leaving hung connections to the BMC web interface. The monarch BMC must be rebooted to recover from this situation. Other BMC management is not impacted. HPE has made the following software update to resolve the vulnerability in HPE Superdome Flex Server: Superdome Flex Server Firmware 3.30.142 or later. **CVE ID : CVE-2021-26581**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04102en_us	H-HPE-SUPE-280421/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
huawei					
ips_module					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-IPS_-280421/1445
ips6000e					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-IPS6-280421/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
ngfw_module					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-NGFW-280421/1447
nip6000e					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-NIP6-280421/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
nip6300					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-NIP6-280421/1449
nip6600					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-NIP6-280421/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
nip6800					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-NIP6-280421/1451
secospace_usg6300					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-SECO-280421/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
secospace_usg6500					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-SECO-280421/1453
secospace_usg6600					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-SECO-280421/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
usg6000e					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-USG6-280421/1455
usg9500					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	H-HUA-USG9-280421/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22312		
intelbras					
win_300					
N/A	14-04-2021	5	The web interface on Intelbras WIN 300 and WRN 342 devices through 2021-01-04 allows remote attackers to discover credentials by reading the def_wirelesspassword line in the HTML source code. **CVE ID : CVE-2021-3017**	https://www.intelbras.com/pt-br/ajuda-download/faq/roteador-wireless-veloz-wrn-342	H-INT-WIN_-280421/1457
wrn_342					
N/A	14-04-2021	5	The web interface on Intelbras WIN 300 and WRN 342 devices through 2021-01-04 allows remote attackers to discover credentials by reading the def_wirelesspassword line in the HTML source code. **CVE ID : CVE-2021-3017**	https://www.intelbras.com/pt-br/ajuda-download/faq/roteador-wireless-veloz-wrn-342	H-INT-WRN_-280421/1458
motorola					
mh702x					
Improper Certificate Validation	13-04-2021	7.5	The Motorola MH702x devices, prior to version 2.0.0.301, do not properly verify the server certificate during communication with the support server which could lead to the communication channel being accessible by an attacker. **CVE ID : CVE-2021-3460**	https://motorolamentor.zendesk.com/hc/en-us/articles/1260804087249	H-MOT-MH70-280421/1459
multilaser					
ac1200					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	14-04-2021	6.8	Multilaser Router AC1200 V02.03.01.45_pt contains a cross-site request forgery (CSRF) vulnerability. An attacker can enable remote access, change passwords, and perform other actions through misconfigured requests, entries, and headers. **CVE ID : CVE-2021-31152**	N/A	H-MUL-AC12-280421/1460
nokia					
g-120w-f					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	3.5	An issue was discovered on Nokia G-120W-F 3FE46606AGAB91 devices. There is Stored XSS in the administrative interface via urlfilter.cgi?add url_address. **CVE ID : CVE-2021-30003**	N/A	H-NOK-G-12-280421/1461
qnap					
nas					
Out-of-bounds Write	14-04-2021	7.5	A stack-based buffer overflow vulnerability has been reported to affect QNAP NAS devices running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. QNAP have already fixed this vulnerability in the following versions: Surveillance Station 5.1.5.4.3 (and later) for ARM CPU NAS (64bit OS) and x86 CPU NAS (64bit OS) Surveillance Station 5.1.5.3.3 (and later) for ARM CPU NAS (32bit OS)	https://www.qnap.com/en/security-advisory/qsa-21-07	H-QNA-NAS-280421/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and x86 CPU NAS (32bit OS) **CVE ID : CVE-2021-28797**		
qualcomm					
aqt1000					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-AQT1-280421/1463
pm8005					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-PM80-280421/1464
pm855					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-PM85-280421/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1892**		
pm855p					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-PM85-280421/1466
pm8998					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-PM89-280421/1467
pmi8998					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-PMI8-280421/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1892		
qat3550					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QAT3-280421/1469
qca1062					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA1-280421/1470
qca1064					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA1-280421/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca2066					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA2-280421/1472
qca6164					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1473
qca6174					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1474
qca6174a					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1475
qca6310					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1476
qca6335					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1477
qca6391					
Improper Input	07-04-2021	7.2	Memory corruption due to improper input validation	https://www.qualco	H-QUA-QCA6-280421/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	mm.com/company/product-security/bulletins/april-2021-bulletin	
qca6420					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1479
qca6430					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA6-280421/1480
qca6595au					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in	https://www.qualcomm.com/company/p	H-QUA-QCA6-280421/1481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	roduct-security/bulletins/april-2021-bulletin	
qca9377					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCA9-280421/1482
qcn7605					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QCN7-280421/1483
qcn7606					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/b	H-QUA-QCN7-280421/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	ulletins/april-2021-bulletin	
qet4100					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QET4-280421/1485
qfe2081fc					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QFE2-280421/1486
qfe2082fc					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/april-2021-	H-QUA-QFE2-280421/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	bulletin	
qfe3100					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QFE3-280421/1488
qfe3440fc					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QFE3-280421/1489
qfe4455fc					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QFE4-280421/1490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1892**		
qln1035bd					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-QLN1-280421/1491
sd835					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SD83-280421/1492
sd845					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SD84-280421/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1892		
sd850					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SD85-280421/1494
sd8c					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SD8C-280421/1495
sd8cx					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SD8C-280421/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdr8150					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SDR8-280421/1497
smb1350					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SMB1-280421/1498
smb1351					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SMB1-280421/1499
smb1380					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SMB1-280421/1500
smb1381					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SMB1-280421/1501
smb1390					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-SMB1-280421/1502
smb2351					
Improper Input	07-04-2021	7.2	Memory corruption due to improper input validation	https://www.qualco	H-QUA-SMB2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	mm.com/company/product-security/bulletins/april-2021-bulletin	280421/1503
wcd9335					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCD9-280421/1504
wcd9340					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCD9-280421/1505
wcd9341					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in	https://www.qualcomm.com/company/p	H-QUA-WCD9-280421/1506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	roduct-security/bulletins/april-2021-bulletin	
wcn3990					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCN3-280421/1507
wcn3998					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCN3-280421/1508
wcn6850					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/b	H-QUA-WCN6-280421/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	ulletins/april-2021-bulletin	
wcn6851					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCN6-280421/1510
wcn6855					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WCN6-280421/1511
wcn6856					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/april-2021-	H-QUA-WCN6-280421/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	bulletin	
wgr7640					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WGR7-280421/1513
wsa8810					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WSA8-280421/1514
wsa8815					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WSA8-280421/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1892**		
wtr5975					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	H-QUA-WTR5-280421/1516
skyworthdigital					
rn510					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2021	3.5	Skyworth Digital Technology RN510 V.3.1.0.4 is affected by an incorrect access control vulnerability in/cgi-bin/test_version.asp. If Wi-Fi is connected but an unauthenticated user visits a URL, the SSID password and web UI password may be disclosed. **CVE ID : CVE-2021-25326**	N/A	H-SKY-RN51-280421/1517
Cross-Site Request Forgery (CSRF)	09-04-2021	4.3	Skyworth Digital Technology RN510 V.3.1.0.4 contains a cross-site request forgery (CSRF) vulnerability in /cgi-bin/net-routeadd.asp and /cgi-bin/sec-urlfilter.asp. Missing CSRF protection in devices can lead to XSRF, as the above pages are vulnerable to cross-site scripting (XSS).	N/A	H-SKY-RN51-280421/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25327		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2021	6.5	Skyworth Digital Technology RN510 V.3.1.0.4 RN510 V.3.1.0.4 contains a buffer overflow vulnerability in /cgi-bin/app-staticIP.asp. An authenticated attacker can send a specially crafted request to endpoint which can lead to a denial of service (DoS) or possible code execution on the device. **CVE ID : CVE-2021-25328**	N/A	H-SKY-RN51-280421/1519
tenda					
g1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"qosIndex "request. This occurs because the "formQOSRuleDel" function directly passes the parameter "qosIndex" to strcpy without limit. **CVE ID : CVE-2021-27705**	N/A	H-TEN-G1-280421/1520
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware version V15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"IPMacBindIndex "request. This occurs because the "formIPMacBindDel"	N/A	H-TEN-G1-280421/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function directly passes the parameter "IPMacBindIndex" to strcpy without limit. **CVE ID : CVE-2021-27706**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"portMappingIndex "request. This occurs because the "formDelPortMapping" function directly passes the parameter "portMappingIndex" to strcpy without limit. **CVE ID : CVE-2021-27707**	N/A	H-TEN-G1-280421/1522
g3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"qosIndex "request. This occurs because the "formQOSRuleDel" function directly passes the parameter "qosIndex" to strcpy without limit. **CVE ID : CVE-2021-27705**	N/A	H-TEN-G3-280421/1523
Buffer Copy without Checking Size of Input ('Classic Buffer	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware version V15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a	N/A	H-TEN-G3-280421/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			crafted action/"IPMacBindIndex "request. This occurs because the "formIPMacBindDel" function directly passes the parameter "IPMacBindIndex" to strcpy without limit. **CVE ID : CVE-2021-27706**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"portMappingIndex "request. This occurs because the "formDelPortMapping" function directly passes the parameter "portMappingIndex" to strcpy without limit. **CVE ID : CVE-2021-27707**	N/A	H-TEN-G3-280421/1525
terra-master					
f2-210					
Incorrect Authorization	03-04-2021	7.5	TerraMaster F2-210 devices through 2021-04-03 use UPnP to make the admin web server accessible over the Internet on TCP port 8181, which is arguably inconsistent with the "It is only available on the local network" documentation. NOTE: manually editing /etc/upnp.json provides a partial but undocumented workaround.	N/A	H-TER-F2-2-280421/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30127		
totolink					
a720r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS. **CVE ID : CVE-2021-27708**	N/A	H-TOT-A720-280421/1527
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "ip" parameter is directly passed to the	N/A	H-TOT-A720-280421/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker, allowing them to control the "ip" field to attack the OS. **CVE ID : CVE-2021-27710**		
x5000r					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS. **CVE ID : CVE-2021-27708**	N/A	H-TOT-X500-280421/1529
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the	N/A	H-TOT-X500-280421/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function, "ip" parameter is directly passed to the attacker, allowing them to control the "ip" field to attack the OS. **CVE ID : CVE-2021-27710**		
tp-link					
tl-wr2041+					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.8	Buffer Overflow in TP-Link WR2041 v1 firmware for the TL-WR2041+ router allows remote attackers to cause a Denial-of-Service (DoS) by sending an HTTP request with a very long "ssid" parameter to the "/userRpm/popupSiteSurveyRpm.html" webpage, which crashes the router. **CVE ID : CVE-2021-26827**	N/A	H-TP--TL-W-280421/1531
tl-wr802n					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-04-2021	9.3	TP-Link TL-WR802N(US), Archer_C50v5_US v4_200 <= 2020.06 contains a buffer overflow vulnerability in the httpd process in the body message. The attack vector is: The attacker can get shell of the router by sending a message through the network, which may lead to remote code execution. **CVE ID : CVE-2021-29302**	https://static.tp-link.com/beta/2021/202103/20210319/TL-WR802Nv4_US_0.9.1_3.17_up_boot[210317-rel64474].zip, https://www.tp-link.com/us/support/download/tl-wr802n/#	H-TP--TL-W-280421/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Firmware	
tl-xdr1850					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	H-TP--TL-X-280421/1533
tl-xdr1860					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-	H-TP--TL-X-280421/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	
tl-xdr3230					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	H-TP--TL-X-280421/1535
tl-xdr3250					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 <	https://service.tp-link.com.cn/detail_d	H-TP--TL-X-280421/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	ownload_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	
tl-xdr5430					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.c	H-TP--TL-X-280421/1537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	n/detail_download_8720.html	
tl-xdr6060					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	H-TP--TL-X-280421/1538
zte					
zxa10_c300m					
Uncontrolled Resource Consumption	09-04-2021	5	A ZTE product has a configuration error vulnerability. Because a certain port is open by default, an attacker can consume system processing resources by flushing a large number of packets to the port, and successfully exploiting this	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014784	H-ZTE-ZXA1-280421/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could reduce system processing capabilities. This affects: ZXA10 C300M all versions up to V4.3P8. **CVE ID : CVE-2021-21728**		
zxcloud_irai					
Cross-Site Request Forgery (CSRF)	13-04-2021	5.8	A CSRF vulnerability exists in the management page of a ZTE product.The vulnerability is caused because the management page does not fully verify whether the request comes from a trusted user. The attacker could submit a malicious request to the affected device to delete the data. This affects: ZXCLOUD iRAI All versions up to KVM-ProductV6.03.04 **CVE ID : CVE-2021-21731**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014824	H-ZTE-ZXCL-280421/1540
zxhn_h108n					
Cross-Site Request Forgery (CSRF)	13-04-2021	4.3	Some ZTE products have CSRF vulnerability. Because some pages lack CSRF random value verification, attackers could perform illegal authorization operations by constructing messages.This affects: ZXHN H168N V3.5.0_EG1T5_TE, V2.5.5, ZXHN H108N V2.5.5_BTMT1 **CVE ID : CVE-2021-21729**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014904	H-ZTE-ZXHN-280421/1541
zxhn_h168n					
Cross-Site Request	13-04-2021	4.3	Some ZTE products have CSRF vulnerability.	https://support.zte.c	H-ZTE-ZXHN-280421/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Because some pages lack CSRF random value verification, attackers could perform illegal authorization operations by constructing messages.This affects: ZXHN H168N V3.5.0_EG1T5_TE, V2.5.5, ZXHN H108N V2.5.5_BTMT1 **CVE ID : CVE-2021-21729**	om.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014904	
Operating System					
apple					
ipad_os					
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1753**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1543
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-IPAD-280421/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1545
Out-of-bounds Read	02-04-2021	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1794**	https://support.apple.com/en-us/HT212146	O-APP-IPAD-280421/1546
Out-of-bounds Write	02-04-2021	7.5	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution.	https://support.apple.com/en-us/HT212146	O-APP-IPAD-280421/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1795		
Out-of-bounds Write	02-04-2021	7.5	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1796**	https://support.apple.com/en-us/HT212146	O-APP-IPAD-280421/1548
N/A	02-04-2021	2.1	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to read arbitrary files. **CVE ID : CVE-2021-1797**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1549
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-	O-APP-IPAD-280421/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ports on arbitrary servers. **CVE ID : CVE-2021-1799**	us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1801**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1551
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://su	O-APP-IPAD-280421/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	pport.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1844**	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223, https://support.apple.com/en-us/HT212220, https://support.apple.com/en-us/HT212221	O-APP-IPAD-280421/1553
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1870		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	4.3	This issue was addressed by improved management of object lifetimes. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3. Processing maliciously crafted web content may lead to universal cross site scripting. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1879**	https://support.apple.com/en-us/HT212256, https://support.apple.com/en-us/HT212257, https://support.apple.com/en-us/HT212258	O-APP-IPAD-280421/1555
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1871**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1556
ipados					
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-IPAD-280421/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1743**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1558
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-IPAD-280421/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1744	us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1745**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1560
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1561
Out-of-	02-04-2021	6.8	An out-of-bounds write was addressed with	https://support.appl	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	e.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1562
Improper Input Validation	02-04-2021	6.8	A validation issue was addressed with improved input sanitization. This issue is fixed in tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2021-1748**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1563
Improper Privilege Management	02-04-2021	9.3	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application may be able to execute	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-IPAD-280421/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2021-1750**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1565
N/A	02-04-2021	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker with physical access to a device may be able to see private contact information. **CVE ID : CVE-2021-1756**	https://support.apple.com/en-us/HT212146	O-APP-IPAD-280421/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1567
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1568
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue	https://support.apple.com/en-	O-APP-IPAD-280421/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1759**	us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2021	9.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution. **CVE ID : CVE-2021-1763**		
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1572
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	9.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2021-1767**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1574
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1768**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1575
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2021-1769**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-IPAD-280421/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1577
N/A	02-04-2021	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1578
N/A	02-04-2021	6.8	This issue was addressed	https://su	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	pport.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1579
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2021-1776**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1580
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update	https://support.apple.com/en-us/HT212	O-APP-IPAD-280421/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1582
Improper Initialization	02-04-2021	4.9	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker in a privileged position may be	https://support.apple.com/en-us/HT212146	O-APP-IPAD-280421/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to perform a denial of service attack. **CVE ID : CVE-2021-1780**		
N/A	02-04-2021	4.3	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2021-1781**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPAD-280421/1584
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1585
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update	https://support.apple.com/en-us/HT212146,	O-APP-IPAD-280421/1586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1587
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-	O-APP-IPAD-280421/1588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1589
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://su	O-APP-IPAD-280421/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	7.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2021-1791**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1591
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212	O-APP-IPAD-280421/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPAD-280421/1593
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.appl	O-APP-IPAD-280421/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-1789**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
iphone_os					
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1595
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212	O-APP-IPHO-280421/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1743**	149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1744**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1597
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution. **CVE ID : CVE-2021-1745**		
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1599
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-04-2021	6.8	A validation issue was addressed with improved input sanitization. This issue is fixed in tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2021-1748**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1601
Improper Privilege Management	02-04-2021	9.3	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1750**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1602
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-	O-APP-IPHO-280421/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker with physical access to a device may be able to see private contact information. **CVE ID : CVE-2021-1756**	https://support.apple.com/en-us/HT212146	O-APP-IPHO-280421/1604
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-IPHO-280421/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1606
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1759**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1607
Improper Restriction of Operations within the Bounds of a Memory	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update	https://support.apple.com/en-us/HT212146, https://su	O-APP-IPHO-280421/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2021	9.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1763**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1609
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-IPHO-280421/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1611
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	9.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2021-1767**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1612
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-IPHO-280421/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1768**	e.com/en-us/HT212147	
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2021-1769**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1614
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-IPHO-280421/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1616
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212	O-APP-IPHO-280421/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				148	
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2021-1776**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1618
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1619
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl.	https://support.appl	O-APP-IPHO-280421/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	e.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Initialization	02-04-2021	4.9	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker in a privileged position may be able to perform a denial of service attack. **CVE ID : CVE-2021-1780**	https://support.apple.com/en-us/HT212146	O-APP-IPHO-280421/1621
N/A	02-04-2021	4.3	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2021-1781**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1623
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1624
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue	https://support.apple.com/en-	O-APP-IPHO-280421/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1626
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update	https://support.apple.com/en-us/HT212146, https://su	O-APP-IPHO-280421/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1628
Out-of-bounds Read	02-04-2021	7.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was	https://support.apple.com/en-us/HT212	O-APP-IPHO-280421/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2021-1791**	146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1630
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-IPHO-280421/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1753**	e.com/en-us/HT212147	
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1632
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-IPHO-280421/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Out-of-bounds Read	02-04-2021	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1794**	https://support.apple.com/en-us/HT212146	O-APP-IPHO-280421/1634
Out-of-bounds Write	02-04-2021	7.5	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1795**	https://support.apple.com/en-us/HT212146	O-APP-IPHO-280421/1635
Out-of-bounds Write	02-04-2021	7.5	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1796**	https://support.apple.com/en-us/HT212146	O-APP-IPHO-280421/1636
N/A	02-04-2021	2.1	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to read arbitrary files. **CVE ID : CVE-2021-1797**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-IPHO-280421/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1638
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://su	O-APP-IPHO-280421/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxing policy. **CVE ID : CVE-2021-1801**	pport.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1640
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1844**	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223, https://support.apple.com/en-us/HT212	O-APP-IPHO-280421/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				220, https://support.apple.com/en-us/HT212221	
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1870**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-IPHO-280421/1642
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	4.3	This issue was addressed by improved management of object lifetimes. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3. Processing maliciously crafted web content may lead to universal cross site scripting. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1879**	https://support.apple.com/en-us/HT212256, https://support.apple.com/en-us/HT212257, https://support.apple.com/en-us/HT212258	O-APP-IPHO-280421/1643
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-IPHO-280421/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-IPHO-280421/1645
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina,	https://support.apple.com/en-us/HT212146,	O-APP-IPHO-280421/1646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1871**	https://support.apple.com/en-us/HT212147	
mac_os					
Creation of Temporary File in Directory with Insecure Permissions	15-04-2021	6.8	Adobe Digital Editions version 4.5.11.187245 (and earlier) is affected by a Privilege Escalation vulnerability during installation. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary file system write in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21100**	https://helpx.adobe.com/security/products/Digital-Editions/apsb21-26.html	O-APP-MAC_-280421/1647
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the certification. Exploitation	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-280421/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28545**		
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-280421/1649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-04-2021	6.8	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28548**	https://helpx.adobe.com/security/products/photoshop/apsb21-28.html	O-APP-MAC_-280421/1650
Buffer Copy	15-04-2021	6.8	Adobe Photoshop versions	https://he	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28549**	lpx.adobe.com/security/products/photoshop/apsb21-28.html	280421/1651
mac_os_x					
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1736**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1652
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1737**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1653
Out-of-	02-04-2021	6.8	An out-of-bounds write was addressed with	https://support.appl	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1738**	e.com/en-us/HT212147	280421/1654
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1655
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-MAC_-280421/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1743	us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1744**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1657
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1745**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1658
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This	https://support.appl	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	e.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1659
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1660
Improper Privilege Management	02-04-2021	9.3	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001	https://support.apple.com/en-us/HT212146,	O-APP-MAC_-280421/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1750**	https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.6	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. **CVE ID : CVE-2021-1751**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1662
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-MAC_-280421/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1664
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212	O-APP-MAC_-280421/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1759**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1666
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2021	9.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-MAC_-280421/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1763**	e.com/en-us/HT212147	
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1669
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-MAC_-280421/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	9.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to heap corruption. **CVE ID : CVE-2021-1767**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1671
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1768**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1672
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-MAC_-280421/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1769	us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2021-1771**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1674
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1675
N/A	02-04-2021	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security	https://support.apple.com/en-us/HT212146, https://su	O-APP-MAC_-280421/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1677
N/A	02-04-2021	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted font may lead to	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-1775**		
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2021-1776**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1679
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1681
N/A	02-04-2021	9.3	A logic error in kext loading was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2021-1779**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1682
N/A	02-04-2021	4.3	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A malicious application may	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be able to leak sensitive user information. **CVE ID : CVE-2021-1781**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1684
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1686
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1687
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in	https://support.apple.com/en-	O-APP-MAC_-280421/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1689
Out-of-	02-04-2021	7.1	An out-of-bounds read	https://su	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2021-1791**	pport.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1690
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1691
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur	https://support.apple.com/en-us/HT212	O-APP-MAC_-280421/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1753**	146, https://support.apple.com/en-us/HT212147	
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1693
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2021-1790**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1694
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big	https://support.apple.com/en-	O-APP-MAC_-280421/1695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Privilege Management	02-04-2021	4.6	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1802**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1696
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1805**	https://support.apple.com/en-us/HT212177	O-APP-MAC_-280421/1697
Concurrent	02-04-2021	7.6	A race condition was	https://su	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			addressed with additional validation. This issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1806**	pport.apple.com/en-us/HT212177	280421/1698
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1699
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223, https://su	O-APP-MAC_-280421/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2021-1844**	pport.apple.com/en-us/HT212220, https://support.apple.com/en-us/HT212221	
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1870**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1701
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212	O-APP-MAC_-280421/1702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				148	
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MAC_-280421/1703
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1765**	https://support.apple.com/en-us/HT212147	O-APP-MAC_-280421/1704
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001	https://support.apple.com/en-us/HT212146, https://su	O-APP-MAC_-280421/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1871**	pport.apple.com/en-us/HT212147	
macos					
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1736**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1706
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1737**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1707
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may lead to arbitrary code execution. **CVE ID : CVE-2021-1738**		
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1709
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1743**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1744**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1711
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1745**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1712
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212	O-APP-MACO-280421/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1714
N/A	02-04-2021	4.6	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. **CVE ID : CVE-2021-1751**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1716
Missing Authorization	02-04-2021	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. **CVE ID : CVE-2021-1755**	https://support.apple.com/en-us/HT211931	O-APP-MACO-280421/1717
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-MACO-280421/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1719
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1759**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-MACO-280421/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212147	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2021	9.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1763**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1722
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-MACO-280421/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1724
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	9.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to heap corruption.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1767		
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1768**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1726
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2021-1769**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1727
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. A user that is removed from an iMessage group	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could rejoin the group. **CVE ID : CVE-2021-1771**		
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1729
N/A	02-04-2021	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1731
N/A	02-04-2021	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2021-1775**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1732
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.appl	O-APP-MACO-280421/1733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2021-1776**	e.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1734
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-MACO-280421/1735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	9.3	A logic error in kext loading was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2021-1779**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1736
N/A	02-04-2021	4.3	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2021-1781**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1737
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://su	O-APP-MACO-280421/1738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	pport.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1739
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212	O-APP-MACO-280421/1740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1741
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.appl	O-APP-MACO-280421/1742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e.com/en-us/HT212148	
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1743
Out-of-bounds Read	02-04-2021	7.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-MACO-280421/1744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1791	https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1745
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1753**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1746
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://su	O-APP-MACO-280421/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted font may lead to arbitrary code execution. **CVE ID : CVE-2021-1790**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1748
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-MACO-280421/1749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
N/A	02-04-2021	2.1	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to read arbitrary files. **CVE ID : CVE-2021-1797**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1750
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-MACO-280421/1751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1801**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1752
Improper Privilege Management	02-04-2021	4.6	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1802**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1753
N/A	02-04-2021	4.3	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.0.1. A local application may be able to enumerate the user's iCloud documents.	https://support.apple.com/en-us/HT211931	O-APP-MACO-280421/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1803		
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1805**	https://support.apple.com/en-us/HT212177	O-APP-MACO-280421/1755
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	7.6	A race condition was addressed with additional validation. This issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1806**	https://support.apple.com/en-us/HT212177	O-APP-MACO-280421/1756
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-MACO-280421/1757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1870**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1758
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-MACO-280421/1759
Access of Resource Using	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is	https://support.apple.com/en-	O-APP-MACO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1760
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1765**	https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1761
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-APP-MACO-280421/1762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1871**		
safari					
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-SAFA-280421/1763
tvos					
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-TVOS-280421/1764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1743**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1765
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-TVOS-280421/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1744	us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1767
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-TVOS-280421/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
Improper Input Validation	02-04-2021	6.8	A validation issue was addressed with improved input sanitization. This issue is fixed in tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2021-1748**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1769
Improper Privilege Management	02-04-2021	9.3	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1750**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1770
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update	https://support.apple.com/en-us/HT212	O-APP-TVOS-280421/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1772
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave,	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-TVOS-280421/1773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1759**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147	O-APP-TVOS-280421/1774
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-TVOS-280421/1775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1776
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-TVOS-280421/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2021-1769**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1778
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1779
N/A	02-04-2021	4.3	A logic issue was addressed	https://su	O-APP-TVOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	pport.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	280421/1780
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1781
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS	https://support.apple.com/en-us/HT212	O-APP-TVOS-280421/1782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2021-1776**	146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1783
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-TVOS-280421/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1785
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-TVOS-280421/1786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1787
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-TVOS-280421/1788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1789
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://su	O-APP-TVOS-280421/1790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	7.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2021-1791**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1791
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212	O-APP-TVOS-280421/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1793
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.appl	O-APP-TVOS-280421/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e.com/en-us/HT212148	
N/A	02-04-2021	2.1	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to read arbitrary files. **CVE ID : CVE-2021-1797**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1795
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-TVOS-280421/1796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1801**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1797
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-TVOS-280421/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-TVOS-280421/1799
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://su	O-APP-TVOS-280421/1800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212148	
watchos					
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1742**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1801
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1743**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-WATC-280421/1802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Out-of-bounds Write	02-04-2021	9.3	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1744**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1803
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1746**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1804
Out-of-	02-04-2021	6.8	An out-of-bounds write	https://su	O-APP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2021-1747**	pport.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	WATC-280421/1805
Improper Input Validation	02-04-2021	6.8	A validation issue was addressed with improved input sanitization. This issue is fixed in tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2021-1748**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1806
Improper Privilege Management	02-04-2021	9.3	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212	O-APP-WATC-280421/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-1750**	149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1754**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1808
Out-of-bounds Read	02-04-2021	4.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1757**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.appl	O-APP-WATC-280421/1809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1758**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1810
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	4.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application could execute arbitrary code leading to compromise of user information. **CVE ID : CVE-2021-1760**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-WATC-280421/1811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
Use After Free	02-04-2021	5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1764**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1812
N/A	02-04-2021	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1766**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-WATC-280421/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
N/A	02-04-2021	2.1	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2021-1769**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1814
Out-of-bounds Write	02-04-2021	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2021-1772**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1815
N/A	02-04-2021	4.3	A logic issue was addressed	https://su	O-APP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1773**	pport.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	WATC-280421/1816
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1774**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1817
Out-of-bounds Write	02-04-2021	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS	https://support.apple.com/en-us/HT212	O-APP-WATC-280421/1818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2021-1776**	146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1777**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1819
Out-of-bounds Read	02-04-2021	4.3	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001	https://support.apple.com/en-us/HT212146, https://support.appl	O-APP-WATC-280421/1820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service. **CVE ID : CVE-2021-1778**	e.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2021	6.9	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1782**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1821
N/A	02-04-2021	6.8	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149,	O-APP-WATC-280421/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1783**	https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1785**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1823
N/A	02-04-2021	4.9	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files. **CVE ID : CVE-2021-1786**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-	O-APP-WATC-280421/1824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212147, https://support.apple.com/en-us/HT212148	
Improper Privilege Management	02-04-2021	4.6	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-1787**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1825
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://su	O-APP-WATC-280421/1826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Out-of-bounds Read	02-04-2021	7.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory. **CVE ID : CVE-2021-1791**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1827
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2021-1792**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212	O-APP-WATC-280421/1828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				147, https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	5	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2021-1761**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1829
N/A	02-04-2021	6.8	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1793**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.appl	O-APP-WATC-280421/1830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e.com/en-us/HT212148	
N/A	02-04-2021	2.1	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to read arbitrary files. **CVE ID : CVE-2021-1797**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1831
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147,	O-APP-WATC-280421/1832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1801**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1833
N/A	02-04-2021	7.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2021-1818**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-	O-APP-WATC-280421/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212148	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1844**	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223, https://support.apple.com/en-us/HT212220, https://support.apple.com/en-us/HT212221	O-APP-WATC-280421/1835
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	4.3	This issue was addressed by improved management of object lifetimes. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3. Processing maliciously crafted web content may lead to universal cross site scripting. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1879**	https://support.apple.com/en-us/HT212256, https://support.apple.com/en-us/HT212257, https://support.apple.com/en-us/HT212258	O-APP-WATC-280421/1836
Out-of-bounds Read	02-04-2021	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security	https://support.apple.com/en-us/HT212146, https://su	O-APP-WATC-280421/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-1741**	pport.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-APP-WATC-280421/1838
asus					
asmb8-ikvm_firmware					
Buffer Copy without	06-04-2021	4	The Radius configuration function in ASUS BMC's	https://www.twcert	O-ASU-ASMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/1839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28176**	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1840
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-ASMB-280421/1841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The UEFI configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	https://www.twcert.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-ASMB-280421/1843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Web service. **CVE ID : CVE-2021-28179**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	https://www.twcert.org.tw/tw/cp-132-4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-ASMB-280421/1845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28182**	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1846
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1847
Buffer Copy without Checking Size	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web	https://www.asus.com/conte	O-ASU-ASMB-280421/1848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4554-10a74-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28185**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4555-3c7c3-1.html	O-ASU-ASMB-280421/1849
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-ASMB-280421/1850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-ASMB-280421/1852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28188	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1853
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	https://www.twcert.org.tw/tw/cp-132-4573-aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-ASMB-280421/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28204**	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1855
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28205**	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1856
asmb9-ikvm_firmware					
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.twcert.org.tw/tw	O-ASU-ASMB-280421/1857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-ASMB-280421/1858
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-ASMB-280421/1859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1860
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-ASMB-280421/1861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28194	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1862
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-	O-ASU-ASMB-280421/1863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1864
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1865
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information	https://www.asus.com/content/ASUS-	O-ASU-ASMB-280421/1866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-ASMB-280421/1867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	O-ASU-ASMB-280421/1868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1869
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-ASMB-280421/1870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-ASMB-280421/1871
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ASMB-280421/1872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-ASMB-280421/1873
e700_g4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1874
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	O-ASU-E700-280421/1875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-E700-280421/1876
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.c	O-ASU-E700-280421/1877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-E700-280421/1879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-E700-280421/1880
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-E700-280421/1883
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	O-ASU-E700-280421/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1885
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	O-ASU-E700-280421/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1887
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-E700-280421/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-E700-280421/1889
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-E700-280421/1890
esc4000_dhd_g4_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-ESC4-280421/1892
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	O-ASU-ESC4-280421/1893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1894
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	O-ASU-ESC4-280421/1895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1896
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-ESC4-280421/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1898
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1899
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-ESC4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/1900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-ESC4-280421/1901
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-ESC4-280421/1902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1903
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	O-ASU-ESC4-280421/1904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-ESC4-280421/1905
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-ESC4-280421/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-ESC4-280421/1907
esc4000_g4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-ESC4-280421/1909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-ESC4-280421/1910
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	O-ASU-ESC4-280421/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	O-ASU-ESC4-280421/1913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-ESC4-280421/1914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-ESC4-280421/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-ESC4-280421/1917
Buffer Copy	06-04-2021	4	The CD media	https://w	O-ASU-ESC4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/1918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1919
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-ESC4-280421/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1921
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-ESC4-280421/1922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1923
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-ESC4-280421/1924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
esc4000_g4x_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1925
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-ESC4-280421/1926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-ESC4-280421/1927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1928
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	O-ASU-ESC4-280421/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1930
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-ESC4-280421/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1932
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-ESC4-280421/1933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-ESC4-280421/1934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-ESC4-280421/1935
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	O-ASU-ESC4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/1936
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC4-280421/1937
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	O-ASU-ESC4-280421/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-ESC4-280421/1939
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	O-ASU-ESC4-280421/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-ESC4-280421/1941
esc8000_g4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-ESC8-280421/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-ESC8-280421/1943
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-ESC8-280421/1944
Buffer Copy	06-04-2021	4	The SMTP configuration	https://w	O-ASU-ESC8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	ww.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/1945
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1946
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4565-59c97-	O-ASU-ESC8-280421/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-ESC8-280421/1948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-	O-ASU-ESC8-280421/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28197**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-ESC8-280421/1951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-ESC8-280421/1952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1953
Buffer Copy without	06-04-2021	4	The Service configuration-2 function in ASUS BMC's	https://www.asus.c	O-ASU-ESC8-280421/1954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1955
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-ESC8-280421/1956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1957
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-ESC8-280421/1958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
esc8000_g4/10g_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-ESC8-280421/1960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-ESC8-280421/1961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1962
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-ESC8-280421/1963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1964
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-ESC8-280421/1965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1966
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-ESC8-280421/1967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28198	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-ESC8-280421/1968
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-	O-ASU-ESC8-280421/1969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1970
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-ESC8-280421/1971
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record	https://www.twcert.org.tw/tw	O-ASU-ESC8-280421/1972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-ESC8-280421/1973
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://w	O-ASU-ESC8-280421/1974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-ESC8-280421/1975
knpa-u16_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-KNPA-280421/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28190**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-KNPA-280421/1977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-	O-ASU-KNPA-280421/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1979
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1980
Buffer Copy without Checking Size	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-KNPA-280421/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-KNPA-280421/1982
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://w	O-ASU-KNPA-280421/1983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-KNPA-280421/1985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28199	ww.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-KNPA-280421/1986
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/call	O-ASU-KNPA-280421/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1988
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1989
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not	https://www.asus.com/content/ASUS-	O-ASU-KNPA-280421/1990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-KNPA-280421/1991
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-KNPA-280421/1992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28209**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
pro_e800_g4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/1993
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-PRO_-280421/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28191	ww.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-PRO_-280421/1995
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-PRO_-280421/1996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/1997
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/1998
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate	https://www.asus.com/content/ASUS-	O-ASU-PRO_-280421/1999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/2000
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.c	O-ASU-PRO_-280421/2001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-PRO_-280421/2002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-PRO_-280421/2003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/2004
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/2005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-PRO_-280421/2006
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-PRO_-280421/2007
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4578-	O-ASU-PRO_-280421/2008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-PRO_-280421/2009
rs100-e10-pi2_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.c	O-ASU-RS10-280421/2010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS10-280421/2011
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-RS10-280421/2012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2013
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2015
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS10-280421/2016
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4567-	O-ASU-RS10-280421/2017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2018
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS10-280421/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS10-280421/2020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://w	O-ASU-RS10-280421/2021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2022
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2023
Improper	06-04-2021	6.8	The specific function in	https://w	O-ASU-RS10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	280421/2024
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS10-280421/2025
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS10-280421/2026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs300-e10-ps4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS30-280421/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS30-280421/2029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS30-280421/2030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2031
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2032
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-RS30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	280421/2033
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2034
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4568-627f7-	O-ASU-RS30-280421/2035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS30-280421/2036
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS30-280421/2037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28200**	us/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	O-ASU-RS30-280421/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2040
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS30-280421/2041
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-RS30-280421/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS30-280421/2043
rs300-e10-rs4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-	O-ASU-RS30-280421/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS30-280421/2045
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS30-280421/2046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	us/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2047
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS30-280421/2048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS30-280421/2050
Buffer Copy without	06-04-2021	4	The Active Directory configuration function in	https://www.twcert	O-ASU-RS30-280421/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2052
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS30-280421/2053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS30-280421/2054
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-	O-ASU-RS30-280421/2055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28201	d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2056
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS30-280421/2057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS30-280421/2058
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS30-280421/2059
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete	https://www.asus.com/conte	O-ASU-RS30-280421/2060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs500-e9-ps4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS50-280421/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS50-280421/2064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28193	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS50-280421/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS50-280421/2067
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2068
Buffer Copy without Checking Size	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS50-280421/2070
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS50-280421/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2072
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	O-ASU-RS50-280421/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2074
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-	O-ASU-RS50-280421/2075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2076
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2077
rs500-e9-rs4_firmware					
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS50-280421/2079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS50-280421/2080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS50-280421/2082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28194	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2083
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-	O-ASU-RS50-280421/2084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2086
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information	https://www.asus.com/content/ASUS-	O-ASU-RS50-280421/2087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS50-280421/2088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	O-ASU-RS50-280421/2089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2090
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS50-280421/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS50-280421/2092
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2094
rs500-e9-rs4-u_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2095
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	O-ASU-RS50-280421/2096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.c	O-ASU-RS50-280421/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS50-280421/2100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS50-280421/2101
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS50-280421/2104
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	O-ASU-RS50-280421/2105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2108
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2110
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2111
rs500a-e10-ps4_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2112
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS50-280421/2113
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	O-ASU-RS50-280421/2114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	O-ASU-RS50-280421/2116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2117
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2120
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/2121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS50-280421/2122
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS50-280421/2123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2124
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS50-280421/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS50-280421/2126
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS50-280421/2127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2128
rs500a-e10-rs4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS50-280421/2130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2131
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	O-ASU-RS50-280421/2132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2133
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	O-ASU-RS50-280421/2134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS50-280421/2135
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS50-280421/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2137
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS50-280421/2138
Buffer Copy	06-04-2021	4	The CD media	https://w	O-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/2139
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2140
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS50-280421/2141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2142
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS50-280421/2143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2144
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS50-280421/2145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
rs500a-e9_rs4_u_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2146
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS50-280421/2147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2148
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2149
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	O-ASU-RS50-280421/2150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS50-280421/2152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS50-280421/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS50-280421/2155
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS50-280421/2156
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	O-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/2157
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2158
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	O-ASU-RS50-280421/2159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS50-280421/2160
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS50-280421/2161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2162
rs500a-e9-ps4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS50-280421/2163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS50-280421/2164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2165
Buffer Copy	06-04-2021	4	The SMTP configuration	https://w	O-ASU-RS50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	ww.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/2166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2167
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4565-59c97-	O-ASU-RS50-280421/2168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS50-280421/2169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS50-280421/2170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28197**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2171
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS50-280421/2172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS50-280421/2173
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2174
Buffer Copy without	06-04-2021	4	The Service configuration-2 function in ASUS BMC's	https://www.asus.c	O-ASU-RS50-280421/2175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2176
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS50-280421/2177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-RS50-280421/2179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs500a-e9-rs4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS50-280421/2181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS50-280421/2182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2183
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-RS50-280421/2184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2185
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS50-280421/2186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2187
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS50-280421/2188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28198	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS50-280421/2189
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-	O-ASU-RS50-280421/2190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS50-280421/2192
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record	https://www.twcert.org.tw/tw	O-ASU-RS50-280421/2193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS50-280421/2194
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://w	O-ASU-RS50-280421/2195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS50-280421/2196
rs520-e9-rs12-e_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS52-280421/2197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28190**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS52-280421/2198
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-	O-ASU-RS52-280421/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2201
Buffer Copy without Checking Size	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-RS52-280421/2202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS52-280421/2203
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://w	O-ASU-RS52-280421/2204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2205
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-RS52-280421/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28199	ww.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS52-280421/2207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/call	O-ASU-RS52-280421/2208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2210
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not	https://www.asus.com/content/ASUS-	O-ASU-RS52-280421/2211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2212
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS52-280421/2213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28209**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs520-e9-rs8_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2214
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-RS52-280421/2215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28191	ww.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS52-280421/2216
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS52-280421/2217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2218
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2219
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate	https://www.asus.com/content/ASUS-	O-ASU-RS52-280421/2220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.c	O-ASU-RS52-280421/2222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS52-280421/2223
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-RS52-280421/2224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2225
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS52-280421/2227
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS52-280421/2228
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4578-	O-ASU-RS52-280421/2229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS52-280421/2230
rs700-e9-rs12_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.c	O-ASU-RS70-280421/2231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS70-280421/2232
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-RS70-280421/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2234
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2236
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS70-280421/2237
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4567-	O-ASU-RS70-280421/2238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2239
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS70-280421/2240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS70-280421/2241
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://w	O-ASU-RS70-280421/2242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2243
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2244
Improper	06-04-2021	6.8	The specific function in	https://w	O-ASU-RS70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	280421/2245
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2246
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS70-280421/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs700-e9-rs4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2248
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS70-280421/2249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS70-280421/2250
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS70-280421/2251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2252
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2253
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-RS70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	280421/2254
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2255
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4568-627f7-	O-ASU-RS70-280421/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS70-280421/2257
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS70-280421/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28200**	us/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2259
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	O-ASU-RS70-280421/2260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2261
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS70-280421/2262
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-RS70-280421/2263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS70-280421/2264
rs700a-e9-rs12v2_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-	O-ASU-RS70-280421/2265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS70-280421/2266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS70-280421/2267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	us/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2268
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS70-280421/2269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS70-280421/2271
Buffer Copy without	06-04-2021	4	The Active Directory configuration function in	https://www.twcert	O-ASU-RS70-280421/2272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2273
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS70-280421/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS70-280421/2275
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-	O-ASU-RS70-280421/2276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28201	d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2277
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS70-280421/2278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS70-280421/2279
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2280
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete	https://www.asus.com/conte	O-ASU-RS70-280421/2281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs700a-e9-rs4_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2282
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS70-280421/2283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS70-280421/2284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS70-280421/2285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28193	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2286
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS70-280421/2287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS70-280421/2288
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2289
Buffer Copy without Checking Size	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-RS70-280421/2290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS70-280421/2291
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS70-280421/2292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	O-ASU-RS70-280421/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2295
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-	O-ASU-RS70-280421/2296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2297
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS70-280421/2298
rs700a-e9-rs4v2_firmware					
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page	https://www.twcert.org.tw/tw	O-ASU-RS70-280421/2299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			(Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS70-280421/2300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS70-280421/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2302
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS70-280421/2303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28194	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-	O-ASU-RS70-280421/2305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2306
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2307
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information	https://www.asus.com/content/ASUS-	O-ASU-RS70-280421/2308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS70-280421/2309
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	O-ASU-RS70-280421/2310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2311
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS70-280421/2312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS70-280421/2313
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS70-280421/2314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS70-280421/2315
rs720-e9-rs12-e_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2316
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not	https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2318
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.c	O-ASU-RS72-280421/2319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2320
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS72-280421/2321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS72-280421/2322
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS72-280421/2325
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.asus.com/content/ASUS-Product-	O-ASU-RS72-280421/2326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2327
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw	O-ASU-RS72-280421/2328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2329
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-RS72-280421/2330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2331
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS72-280421/2332
rs720-e9-rs24-u_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2333
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2334
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string	https://www.asus.com/content/ASUS-Product-	O-ASU-RS72-280421/2335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2336
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/conte	O-ASU-RS72-280421/2337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2338
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-RS72-280421/2339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2340
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2341
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	280421/2342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS72-280421/2343
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS72-280421/2344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2345
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28206	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS72-280421/2347
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS72-280421/2348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS72-280421/2349
rs720-e9-rs8-g_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2351
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2352
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4563-	O-ASU-RS72-280421/2353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2354
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/conte	O-ASU-RS72-280421/2355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS72-280421/2356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS72-280421/2357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2358
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS72-280421/2359
Buffer Copy	06-04-2021	4	The CD media	https://w	O-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	280421/2360
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2361
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS72-280421/2362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2363
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS72-280421/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28207	us/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2365
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS72-280421/2366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4579-c8827-1.html	
rs720a-e9-rs12v2_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2369
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2370
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the	https://www.twcert.org.tw/tw/cp-132-4564-	O-ASU-RS72-280421/2371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2372
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS72-280421/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2374
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS72-280421/2375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS72-280421/2376
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS72-280421/2377
Buffer Copy	06-04-2021	4	The Service configuration-1	https://w	O-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/2378
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2379
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4576-422ac-	O-ASU-RS72-280421/2380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS72-280421/2381
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28208	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS72-280421/2383
rs720a-e9-rs24-e_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-RS72-280421/2384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2385
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2386
Buffer Copy	06-04-2021	4	The SMTP configuration	https://w	O-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	ww.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/2387
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2388
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4565-59c97-	O-ASU-RS72-280421/2389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS72-280421/2390
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28197**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS72-280421/2393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS72-280421/2394
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2395
Buffer Copy without	06-04-2021	4	The Service configuration-2 function in ASUS BMC's	https://www.asus.c	O-ASU-RS72-280421/2396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	om/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2397
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS72-280421/2398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2399
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-RS72-280421/2400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs720a-e9-rs24v2_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-RS72-280421/2402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2404
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-RS72-280421/2405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2406
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-RS72-280421/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2408
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS72-280421/2409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28198	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS72-280421/2410
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-	O-ASU-RS72-280421/2411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2412
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2413
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record	https://www.twcert.org.tw/tw	O-ASU-RS72-280421/2414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS72-280421/2415
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://w	O-ASU-RS72-280421/2416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS72-280421/2417
rs720q-e9-rs24-s_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-RS72-280421/2418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28190**	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2419
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-	O-ASU-RS72-280421/2420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2421
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2422
Buffer Copy without Checking Size	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-RS72-280421/2423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS72-280421/2424
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://w	O-ASU-RS72-280421/2425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-RS72-280421/2427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28199	ww.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS72-280421/2428
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/call	O-ASU-RS72-280421/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2430
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2431
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not	https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2433
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-RS72-280421/2434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28209**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rs720q-e9-rs8_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2435
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-RS72-280421/2436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28191	ww.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-RS72-280421/2437
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-RS72-280421/2438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2439
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2440
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate	https://www.asus.com/content/ASUS-	O-ASU-RS72-280421/2441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2442
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.c	O-ASU-RS72-280421/2443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-RS72-280421/2444
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-RS72-280421/2445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2446
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2448
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-RS72-280421/2449
Improper Limitation of a Pathname to a Restricted	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4578-	O-ASU-RS72-280421/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-RS72-280421/2451
rs720q-e9-rs8-s_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.c	O-ASU-RS72-280421/2452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-RS72-280421/2453
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-RS72-280421/2454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2457
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-RS72-280421/2458
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4567-	O-ASU-RS72-280421/2459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2460
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-RS72-280421/2461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	pport/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-RS72-280421/2462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://w	O-ASU-RS72-280421/2463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2464
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2465
Improper	06-04-2021	6.8	The specific function in	https://w	O-ASU-RS72-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	280421/2466
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-RS72-280421/2467
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-RS72-280421/2468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
rt-ac1750_b1_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2469
rt-ac1900_firmware					
Excessive	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-	https://www.asus.c	O-ASU-RT-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Iteration			AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	280421/2470
rt-ac1900p_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/,	O-ASU-RT-A-280421/2471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac1900u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2472
rt-ac2900_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/,	O-ASU-RT-A-280421/2473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac3100_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/	O-ASU-RT-A-280421/2474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				HelpDesk_download/	
rt-ac5300_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2475
rt-ac58u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-	O-ASU-RT-A-280421/2476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac65u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2477
rt-ac66u_b1_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2478
rt-ac68p_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/Hel	O-ASU-RT-A-280421/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	pDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac68r_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2480
rt-ac68rw_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or <	https://www.asus.com/supportonly/RT-AC3100/H	O-ASU-RT-A-280421/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	elpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac68u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/suppo	O-ASU-RT-A-280421/2482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			set. **CVE ID : CVE-2021-3128**	rtonly/RT-AC1900P/HelpDesk_download/	
rt-ac68w_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2483
rt-ac85u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Netw	O-ASU-RT-A-280421/2484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	orking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ac86u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rt-ac88u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2486
rt-ax3000_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-	O-ASU-RT-A-280421/2487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax55_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2488
rt-ax56u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware <	https://www.asus.com/supportonly/RT-	O-ASU-RT-A-280421/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax58u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.c	O-ASU-RT-A-280421/2490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax68u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2491
rt-ax82u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.c	O-ASU-RT-A-280421/2492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	om/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
rt-ax86u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download	O-ASU-RT-A-280421/2493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/	
rt-ax88u_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	https://www.asus.com/supportonly/RT-AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	O-ASU-RT-A-280421/2494
ws_c422_pro/se_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-WS_C-280421/2495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28190	https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-WS_C-280421/2496
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-WS_C-280421/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2499
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length	https://www.twcert.org.tw/tw/cp-132-4565-	O-ASU-WS_C-280421/2500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-WS_C-280421/2501
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/conte	O-ASU-WS_C-280421/2502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2503
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-WS_C-280421/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-WS_C-280421/2505
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2506
Buffer Copy	06-04-2021	4	The Service configuration-2	https://w	O-ASU-WS_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	ww.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	280421/2507
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2508
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-WS_C-280421/2509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2510
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-WS_C-280421/2511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28209	us/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
ws_c621e_sage_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-WS_C-280421/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-WS_C-280421/2514
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2515
Buffer Copy	06-04-2021	4	The specific function in	https://w	O-ASU-WS_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	ww.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/2516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2517
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered	https://www.asus.com/content/ASUS-Product-Security-	O-ASU-WS_C-280421/2518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-	O-ASU-WS_C-280421/2520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28198**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-WS_C-280421/2521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-WS_C-280421/2522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-WS_C-280421/2524
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.twcert	O-ASU-WS_C-280421/2525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-WS_C-280421/2526
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html,	O-ASU-WS_C-280421/2527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-WS_C-280421/2528
ws_x299_pro/se_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-	O-ASU-WS_X-280421/2529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-WS_X-280421/2530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-	O-ASU-WS_X-280421/2531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2533
Buffer Copy without	06-04-2021	4	The Radius configuration function in ASUS BMC's	https://www.twcert	O-ASU-WS_X-280421/2534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-WS_X-280421/2535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html,	O-ASU-WS_X-280421/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2537
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-WS_X-280421/2538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-WS_X-280421/2539
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/su	O-ASU-WS_X-280421/2540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2541
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2542
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get	https://www.asus.com/conte	O-ASU-WS_X-280421/2543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-WS_X-280421/2544
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-WS_X-280421/2545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
z10pe-d16_ws_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	https://www.twcert.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2546
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-	O-ASU-Z10P-280421/2547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28176	Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	O-ASU-Z10P-280421/2548
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The UEFI configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	https://www.twcert.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-Z10P-280421/2549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28179**	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2550
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2551
Buffer Copy without Checking Size	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote	https://www.twcert.org.tw/tw	O-ASU-Z10P-280421/2552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			video configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	/cp-132-4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28182**	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2553
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-Z10P-280421/2554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	ww.twcert.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4554-10a74-1.html	O-ASU-Z10P-280421/2555
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://w	O-ASU-Z10P-280421/2556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28185	ww.twcert.org.tw/tw/cp-132-4555-3c7c3-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	O-ASU-Z10P-280421/2557
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/call	O-ASU-Z10P-280421/2558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28188**	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2560
Improper Neutralization of Special Elements	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not	https://www.twcert.org.tw/tw/cp-132-	O-ASU-Z10P-280421/2561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	4573-aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28204**	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2562
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.c	O-ASU-Z10P-280421/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			means of path traversal to access system files. **CVE ID : CVE-2021-28205**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
z10pr-d16_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28175**	https://www.twcert.org.tw/tw/cp-132-4543-98220-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The DNS configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.twcert.org.tw/tw/cp-132-4544-0a409-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-Z10P-280421/2565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28176	Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The LDAP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28177**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4547-88e43-1.html	O-ASU-Z10P-280421/2566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The UEFI configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28178**	https://www.twcert.org.tw/tw/cp-132-4548-7a2c6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-Z10P-280421/2567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Media support configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28179**	https://www.twcert.org.tw/tw/cp-132-4549-c97ba-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2568
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Audit log configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28180**	https://www.twcert.org.tw/tw/cp-132-4550-5ee8c-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2569
Buffer Copy without Checking Size of Input	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video configuration	https://www.twcert.org.tw/tw/cp-132-	O-ASU-Z10P-280421/2570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28181**	4551-5dd2f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Web Service configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28182**	https://www.twcert.org.tw/tw/cp-132-4552-5b2c4-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2571
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Web License configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert	O-ASU-Z10P-280421/2572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28183**	.org.tw/tw/cp-132-4553-06ae2-1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28184**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4554-10a74-1.html	O-ASU-Z10P-280421/2573
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-1 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28185**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-Z10P-280421/2574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4555-3c7c3-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28186**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4556-ece3d-1.html	O-ASU-Z10P-280421/2575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new SSL certificate) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28187**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4557-1019f-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28188**	https://www.twcert.org.tw/tw/cp-132-4558-ad16e-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28189**	https://www.twcert.org.tw/tw/cp-132-4559-ad2b5-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2578
Improper Neutralization of Special Elements used in an OS	06-04-2021	6.5	The Web Set Media Image function in ASUS BMC's firmware Web management page does not filter the specific	https://www.twcert.org.tw/tw/cp-132-4573-	O-ASU-Z10P-280421/2579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28203**	aa336-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2021	6.5	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can launch command injection to execute command arbitrary. **CVE ID : CVE-2021-28204**	https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z10P-280421/2580
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete SOL video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to	https://www.twcert.org.tw/tw/cp-132-4575-2e32d-1.html, https://www.asus.com/conte	O-ASU-Z10P-280421/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access system files. **CVE ID : CVE-2021-28205**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
z11pa-d8_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2582
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert	O-ASU-Z11P-280421/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-Z11P-280421/2584
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2587
Buffer Copy without Checking Size of Input ('Classic	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify	https://www.asus.com/content/ASUS-Product-	O-ASU-Z11P-280421/2588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/conte	O-ASU-Z11P-280421/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-Z11P-280421/2591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-Z11P-280421/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2593
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2594
Improper	06-04-2021	6.8	The specific function in	https://w	O-ASU-Z11P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	ww.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/2595
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-Z11P-280421/2596
Improper Limitation of a Pathname to a Restricted Directory	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-	O-ASU-Z11P-280421/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-Z11P-280421/2598
z11pa-d8c_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/conte	O-ASU-Z11P-280421/2599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	nt/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-Z11P-280421/2600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw	O-ASU-Z11P-280421/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2602
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2603
Buffer Copy	06-04-2021	4	The Radius configuration	https://w	O-ASU-Z11P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	ww.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	280421/2604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-Z11P-280421/2605
Buffer Copy without Checking Size of Input ('Classic Buffer	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting	https://www.twcert.org.tw/tw/cp-132-4567-34350-	O-ASU-Z11P-280421/2606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-Z11P-280421/2608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	us/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-Z11P-280421/2609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.c	O-ASU-Z11P-280421/2610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2611
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2612
Improper Limitation of	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web	https://www.asus.c	O-ASU-Z11P-280421/2613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2614
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator	https://www.asus.com/content/ASUS-Product-Security-Advisory/,	O-ASU-Z11P-280421/2615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
z11pa-u12_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-Z11P-280421/2617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			terminate the Web service. **CVE ID : CVE-2021-28191**	us/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-Z11P-280421/2618
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-Z11P-280421/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				om/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2621
Buffer Copy without	06-04-2021	4	The specific function in ASUS BMC's firmware Web	https://www.asus.c	O-ASU-Z11P-280421/2622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	om/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html,	O-ASU-Z11P-280421/2624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-Z11P-280421/2625
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-Z11P-280421/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28200	https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2627
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/su	O-ASU-Z11P-280421/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2629
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-Z11P-280421/2630
Improper Limitation of a Pathname	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get	https://www.twcert.org.tw/tw	O-ASU-Z11P-280421/2631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-Z11P-280421/2632
z11pa-u12/10g-2s_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html,	O-ASU-Z11P-280421/2633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	O-ASU-Z11P-280421/2634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/,	O-ASU-Z11P-280421/2635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Web service. **CVE ID : CVE-2021-28192**	https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2636
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/su	O-ASU-Z11P-280421/2637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				pport/call us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2638
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-Z11P-280421/2639
Buffer Copy without Checking Size	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web	https://www.twcert.org.tw/tw	O-ASU-Z11P-280421/2640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	https://www.twcert.org.tw/tw/cp-132-4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-Z11P-280421/2642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	O-ASU-Z11P-280421/2643
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-	O-ASU-Z11P-280421/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2645
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-Z11P-280421/2646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-Z11P-280421/2647
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2648
Improper Limitation of a Pathname to a	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does	https://www.asus.com/content/ASUS-	O-ASU-Z11P-280421/2649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	
z11pr-d16_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate new certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28190**	https://www.twcert.org.tw/tw/cp-132-4560-2f01f-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2650
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Firmware update function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://w	O-ASU-Z11P-280421/2651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28191**	ww.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4561-062d0-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote video storage function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28192**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4562-4b207-1.html	O-ASU-Z11P-280421/2652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The SMTP configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28193**	https://www.twcert.org.tw/tw/cp-132-4563-e4092-1.html, https://www.asus.com/content/ASUS-Product-Security-	O-ASU-Z11P-280421/2653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Remote image configuration setting) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28194**	https://www.twcert.org.tw/tw/cp-132-4564-7ef3d-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2654
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28195**	https://www.twcert.org.tw/tw/cp-132-4565-59c97-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/call	O-ASU-Z11P-280421/2655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Generate SSL certificate function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28196**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4566-9154b-1.html	O-ASU-Z11P-280421/2656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Active Directory configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28197**	https://www.twcert.org.tw/tw/cp-132-4567-34350-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2657
Buffer Copy without Checking Size of Input	06-04-2021	4	The Firmware protocol configuration function in ASUS BMC's firmware Web management page does not	https://www.twcert.org.tw/tw/cp-132-	O-ASU-Z11P-280421/2658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28198**	4568-627f7-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The specific function in ASUS BMC's firmware Web management page (Modify user's information function) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28199**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4569-6b391-1.html	O-ASU-Z11P-280421/2659
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The CD media configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission,	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.c	O-ASU-Z11P-280421/2660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28200**	om/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4570-4d216-1.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-1 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28201**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	4	The Service configuration-2 function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service. **CVE ID : CVE-2021-28202**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.twcert.org.tw/tw/cp-132-4571-d454c-1.html,	O-ASU-Z11P-280421/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://www.asus.com/tw/support/callus/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Record video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28206**	https://www.twcert.org.tw/tw/cp-132-4576-422ac-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2663
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get Help file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28207**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4577-60153-1.html	O-ASU-Z11P-280421/2664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Get video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28208**	https://www.twcert.org.tw/tw/cp-132-4578-e5d74-1.html, https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/	O-ASU-Z11P-280421/2665
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	6.8	The specific function in ASUS BMC's firmware Web management page (Delete video file function) does not filter the specific parameter. As obtaining the administrator permission, remote attackers can use the means of path traversal to access system files. **CVE ID : CVE-2021-28209**	https://www.asus.com/content/ASUS-Product-Security-Advisory/, https://www.asus.com/tw/support/callus/, https://www.twcert.org.tw/tw/cp-132-4579-c8827-1.html	O-ASU-Z11P-280421/2666
zenwifi_ax_(xt8)_firmware					
Excessive Iteration	12-04-2021	5	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware <	https://www.asus.com/supportonly/RT-	O-ASU-ZENW-280421/2667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3128**	AC3100/HelpDesk_download/, https://www.asus.com/Networking-IoT-Servers/WiFi-6/All-series/RT-AX55/HelpDesk_BIOS/, https://www.asus.com/supportonly/RT-AC1900P/HelpDesk_download/	
cisco					
ios_xr					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	08-04-2021	7.2	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges on the underlying Linux operating system (OS) of an affected device. This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cmdinj-vsKGherc	O-CIS-IOS_-280421/2668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command. A successful exploit could allow the attacker to execute commands on the underlying Linux OS with root privileges. **CVE ID : CVE-2021-1485**		
rv110w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	O-CIS-RV11-280421/2669
rv130_firmware					
Improper Restriction of Operations within the	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130,	https://tools.cisco.com/security/center/	O-CIS-RV13-280421/2670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**	content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	
rv130w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	O-CIS-RV13-280421/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**		
rv132w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV13-280421/2672
Improper Restriction of Operations	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP)	https://tools.cisco.com/securi	O-CIS-RV13-280421/2673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV13-280421/2674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
rv134w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV13-280421/2675
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-	O-CIS-RV13-280421/2676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV13-280421/2677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rv160_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV16-280421/2678
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV16-280421/2679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV16-280421/2680
Improper Restriction of Operations within the Bounds of a Memory	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV16-280421/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	
rv160w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV16-280421/2682
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory	O-CIS-RV16-280421/2683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV16-280421/2684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV16-280421/2685
rv215w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm	O-CIS-RV21-280421/2686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2021-1459**		
rv260_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2687
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-	O-CIS-RV26-280421/2688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV26-280421/2690
rv260p_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2692
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV26-280421/2694
rv260w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV26-280421/2696
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-RV26-280421/2697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV26-280421/2698
rv340_firmware					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-RV34-280421/2699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**	sb-rv34x-rce-8bfG2h6b	
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2701
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-	O-CIS-RV34-280421/2702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2704
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2705
Improper Restriction of	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based	https://tools.cisco.c	O-CIS-RV34-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	280421/2706
rv340w_firmware					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2708
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2710
Improper Restriction of Operations within the	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco	https://tools.cisco.com/security/center/	O-CIS-RV34-280421/2711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2713
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2714
rv345_firmware					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	https://tools.cisco.com/security/center/content/CiscoSecurit	O-CIS-RV34-280421/2715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1415**	yAdvisory /cisco-sa-sb-rv34x-rce-8bfG2h6b	
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2717
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-RV34-280421/2718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2720
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2722
rv345p_firmware					
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1415		
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1414**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2724
Deserialization of Untrusted Data	08-04-2021	6.5	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b	O-CIS-RV34-280421/2725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. **CVE ID : CVE-2021-1413**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	8.3	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1309**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2726
Improper Restriction of Operations	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP)	https://tools.cisco.com/securi	O-CIS-RV34-280421/2727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1308**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.1	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	O-CIS-RV34-280421/2728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2021-1251**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1472**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2729
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	7.5	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1473**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx	O-CIS-RV34-280421/2730
unified_intelligence_center					
Improper Neutralization of Input During Web Page	08-04-2021	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center Software could allow an	https://tools.cisco.com/security/center/content/Ci	O-CIS-UNIF-280421/2731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1463**	scoSecurityAdvisory/cisco-sa-cuic-xss-U2WTsUg6	
d-link					
dsl-320b-d1					
Out-of-bounds Write	07-04-2021	10	** UNSUPPORTED WHEN ASSIGNED ** D-Link DSL-320B-D1 devices through EU_1.25 are prone to multiple Stack-Based Buffer Overflows that allow unauthenticated remote attackers to take over a device via the login.xgi user and pass parameters. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-26709**	https://www.dlink.com/en/security-bulletin, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10216	O-D-L-DSL--280421/2732
debian					
debian_linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-04-2021	5	A vulnerability in the email parsing module in Clam AntiVirus (ClamAV) Software version 0.103.1 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper variable initialization that may result in an NULL pointer read. An attacker could exploit this vulnerability by sending a crafted email to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition. **CVE ID : CVE-2021-1405**	https://blog.clamav.net/2021/04/clamav-01032-security-patch-release.html	O-DEB-DEBI-280421/2733
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2021	5	In Django 2.2 before 2.2.20, 3.0 before 3.0.14, and 3.1 before 3.1.8, MultiPartParser allowed directory traversal via uploaded files with suitably crafted file names. Built-in upload handlers were not affected by this vulnerability. **CVE ID : CVE-2021-28658**	https://www.djangoproject.com/weblog/2021/apr/06/security-releases/, https://docs.djangoproject.com/en/3.1/releases/security/	O-DEB-DEBI-280421/2734
Incorrect Permission Assignment for Critical Resource	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.13 and 1.32.x through 1.35.x before 1.35.2. When using the MediaWiki API to "protect" a page, a user is	https://phabricator.wikimedia.org/T270713	O-DEB-DEBI-280421/2735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			currently able to protect to a higher level than they currently have permissions for. **CVE ID : CVE-2021-30152**		
Missing Authorization	09-04-2021	4	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. ContentModelChange does not check if a user has correct permissions to create and set the content model of a nonexistent page. **CVE ID : CVE-2021-30155**	https://phabricator.wikimedia.org/T270988	O-DEB-DEBI-280421/2736
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2021	4.3	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. On ChangesList special pages such as Special:RecentChanges and Special:Watchlist, some of the rcfilters-filter-* label messages are output in HTML unescaped, leading to XSS. **CVE ID : CVE-2021-30157**	https://phabricator.wikimedia.org/T278058	O-DEB-DEBI-280421/2737
Improper Authentication	06-04-2021	5	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Blocked users are unable to use Special:ResetTokens. This has security relevance because a blocked user might have accidentally shared a token, or might know that a token has been compromised, and yet is not able to block any	https://phabricator.wikimedia.org/T277009	O-DEB-DEBI-280421/2738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential future use of the token by an unauthorized party. **CVE ID : CVE-2021-30158**		
dell					
wyse_thinos					
Improper Input Validation	02-04-2021	5.8	Dell Wyse ThinOS 8.6 MR9 contains remediation for an improper management server validation vulnerability that could be potentially exploited to redirect a client to an attacker-controlled management server, thus allowing the attacker to change the device configuration or certificate file. **CVE ID : CVE-2021-21532**	https://www.dell.com/support/kbdoc/en-us/000184665/dsa-2021-069-dell-wyse-thinos-8-6-security-update-for-an-improper-management-server-validation-vulnerabilitydsa-2021-069-dell-wyse-thinos-8-6-security-update-for-an-improper-management-server-validation-	O-DEL-WYSE-280421/2739
dlink					
dir-802_firmware					
Improper Neutralization of Special	12-04-2021	5.8	** UNSUPPORTED WHEN ASSIGNED ** An issue was discovered on D-Link DIR-	https://www.dlink.com/en/se	O-DLI-DIR--280421/2740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			802 A1 devices through 1.00b05. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-29379**	curity-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10206	
dir-816_firmware					
Out-of-bounds Write	14-04-2021	7.5	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. Within the handler function of the /goform/addassignment route, a very long text entry for the"'s_ip" and "s_mac" fields could lead to a Stack-Based Buffer Overflow and overwrite the return address. **CVE ID : CVE-2021-27114**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--280421/2741
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. An HTTP request parameter is used in command string construction within the handler function of the /goform/addRouting route. This could lead to Command Injection via Shell Metacharacters. **CVE ID : CVE-2021-27113**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--280421/2742
dir-878_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-04-2021	7.5	An issue was discovered in prog.cgi on D-Link DIR-878 1.30B08 devices. Because strcat is misused, there is a stack-based buffer overflow that does not require authentication. **CVE ID : CVE-2021-30072**	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10217	O-DLI-DIR--280421/2743
fedoraproject					
fedora					
Use After Free	02-04-2021	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1788**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-FED-FEDO-280421/2744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-04-2021	4.3	A port redirection issue was addressed with additional port validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. A malicious website may be able to access restricted ports on arbitrary servers. **CVE ID : CVE-2021-1799**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212148	O-FED-FEDO-280421/2745
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1801**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.apple.com/en-us/HT212	O-FED-FEDO-280421/2746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				148	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2021	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1844**	https://support.apple.com/en-us/HT212222, https://support.apple.com/en-us/HT212223, https://support.apple.com/en-us/HT212220, https://support.apple.com/en-us/HT212221	O-FED-FEDO-280421/2747
Access of Resource Using Incompatible Type ('Type Confusion')	02-04-2021	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2021-1789**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212152, https://support.apple.com/en-us/HT212149, https://support.apple.com/en-us/HT212147, https://support.appl	O-FED-FEDO-280421/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e.com/en-us/HT212148	
N/A	02-04-2021	4.3	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Maliciously crafted web content may violate iframe sandboxing policy. **CVE ID : CVE-2021-1765**	https://support.apple.com/en-us/HT212147	O-FED-FEDO-280421/2749
N/A	02-04-2021	7.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2021-1871**	https://support.apple.com/en-us/HT212146, https://support.apple.com/en-us/HT212147	O-FED-FEDO-280421/2750
Exposure of Sensitive Information to an Unauthorized Actor	01-04-2021	5	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests,	https://curl.se/docs/CVE-2021-22876.html	O-FED-FEDO-280421/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and therefore risks leaking sensitive data to the server that is the target of the second HTTP request. **CVE ID : CVE-2021-22876**		
Authentication Bypass by Spoofing	01-04-2021	4.3	curl 7.63.0 to and including 7.75.0 includes vulnerability that allows a malicious HTTPS proxy to MITM a connection due to bad handling of TLS 1.3 session tickets. When using a HTTPS proxy and TLS 1.3, libcurl can confuse session tickets arriving from the HTTPS proxy but work as if they arrived from the remote server and then wrongly "short-cut" the host handshake. When confusing the tickets, a HTTPS proxy can trick libcurl to use the wrong session ticket resume for the host and thereby circumvent the server TLS certificate check and make a MITM attack to be possible to perform unnoticed. Note that such a malicious HTTPS proxy needs to provide a certificate that curl will accept for the MITMed server for an attack to work - unless curl has been told to ignore the server certificate check. **CVE ID : CVE-2021-22890**	https://curl.se/docs/CVE-2021-22890.html	O-FED-FEDO-280421/2752
Improper Neutralization of Special Elements	08-04-2021	7.2	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch	https://www.openwall.com/lists/oss-	O-FED-FEDO-280421/2753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c. **CVE ID : CVE-2021-29154**	security/2021/04/08/1	
Incorrect Authorization	06-04-2021	5	The Net::Netmask module before 2.0000 for Perl does not properly consider extraneous zero characters at the beginning of an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses. **CVE ID : CVE-2021-29424**	N/A	O-FED-FEDO-280421/2754
NULL Pointer Dereference	07-04-2021	2.1	An issue was discovered in the Linux kernel through 5.11.11. synic_get in arch/x86/kvm/hyperv.c has a NULL pointer dereference for certain accesses to the SynIC Hyper-V context, aka CID-919f4ebc5987. **CVE ID : CVE-2021-30178**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=919f4ebc5987701670e80e31573a58f1f2d2bf918	O-FED-FEDO-280421/2755
Improper Input Validation	15-04-2021	7.1	There's a flaw in the BFD library of binutils in versions before 2.36. An attacker who supplies a crafted file to an application linked with BFD, and using the DWARF functionality, could cause an impact to system	https://bugzilla.redhat.com/show_bug.cgi?id=1947111	O-FED-FEDO-280421/2756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			availability by way of excessive memory consumption. **CVE ID : CVE-2021-3487**		
freebsd					
freebsd					
Double Free	07-04-2021	7.2	In FreeBSD 13.0-STABLE before n245050, 12.2-STABLE before r369525, 13.0-RC4 before p0, and 12.2-RELEASE before p6, listening socket accept filters implementing the accf_create callback incorrectly freed a process supplied argument string. Additional operations on the socket can lead to a double free or use after free. **CVE ID : CVE-2021-29627**	https://security.FreeBSD.org/advisories/FreeBSD-SA-21:09.accept_filter.asc	O-FRE-FREE-280421/2757
Use After Free	07-04-2021	2.1	In FreeBSD 13.0-STABLE before n245117, 12.2-STABLE before r369551, 11.4-STABLE before r369559, 13.0-RC5 before p1, 12.2-RELEASE before p6, and 11.4-RELEASE before p9, copy-on-write logic failed to invalidate shared memory page mappings between multiple processes allowing an unprivileged process to maintain a mapping after it is freed, allowing the process to read private data belonging to other processes or the kernel. **CVE ID : CVE-2021-29626**	https://security.FreeBSD.org/advisories/FreeBSD-SA-21:08.vm.asc	O-FRE-FREE-280421/2758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
genexis					
platinum_4410_firmware					
N/A	13-04-2021	7.5	Genexis PLATINUM 4410 2.1 P4410-V2-1.28 devices allow remote attackers to execute arbitrary code via shell metacharacters to sys_config_valid.xgi, as demonstrated by the sys_config_valid.xgi?exeshell=%60telnetd%20%26%60 URI. **CVE ID : CVE-2021-29003**	N/A	O-GEN-PLAT-280421/2759
google					
android					
Improper Privilege Management	09-04-2021	2.1	A pendingIntent hijacking vulnerability in Create Movie prior to SMR APR-2021 Release 1 in Android O(8.x) and P(9.0), 3.4.81.1 in Android Q(10,0), and 3.6.80.7 in Android R(11.0) allows unprivileged applications to access contact information. **CVE ID : CVE-2021-25357**	https://security.samsungmobile.com/securityUpdate.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2760
Incorrect Default Permissions	09-04-2021	2.1	A vulnerability that stores IMSI values in an improper path prior to SMR APR-2021 Release 1 allows local attackers to access IMSI values without any permission via untrusted applications. **CVE ID : CVE-2021-25358**	https://security.samsungmobile.com/securityUpdate.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2761
Incorrect Default Permissions	09-04-2021	2.1	An improper SELinux policy prior to SMR APR-2021 Release 1 allows local attackers to access AP information without	https://security.samsungmobile.com/securityUpda	O-GOO-ANDR-280421/2762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proper permissions via untrusted applications. **CVE ID : CVE-2021-25359**	te.smsb, https://security.samsungmobile.com/	
Out-of-bounds Write	09-04-2021	7.5	An improper input validation vulnerability in libswmfextractor library prior to SMR APR-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process. **CVE ID : CVE-2021-25360**	https://security.samsungmobile.com/securityUpdate.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2763
Incorrect Authorization	09-04-2021	4.6	Using unsafe PendingIntent in Customization Service prior to version 2.2.02.1 in Android O(8.x), 2.4.03.0 in Android P(9.0), 2.7.02.1 in Android Q(10.0) and 2.9.01.1 in Android R(11.0) allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent. **CVE ID : CVE-2021-25373**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2764
Incorrect Authorization	09-04-2021	5	An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink in versions 2.4.83.9 in Android O(8.1) and below, and 3.9.00.9 in Android P(9.0) and above allows remote attackers to access a user data related with Samsung Account. **CVE ID : CVE-2021-25374**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2765
Improper Privilege	09-04-2021	4.6	Intent redirection in Samsung Experience	https://security.sam	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Service versions 10.8.0.4 in Android P(9.0) below, and 12.2.0.5 in Android Q(10.0) above allows attacker to execute privileged action. **CVE ID : CVE-2021-25377**	sungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	280421/2766
Incorrect Authorization	09-04-2021	7.2	An improper caller check vulnerability in Managed Provisioning prior to SMR APR-2021 Release 1 allows unprivileged application to install arbitrary application, grant device admin permission and then delete several installed application. **CVE ID : CVE-2021-25356**	https://security.samsungmobile.com/securityUpdate.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2767
Incorrect Default Permissions	09-04-2021	4.6	Using unsafe PendingIntent in Samsung Account in versions 10.8.0.4 in Android P(9.0) and below, and 12.1.1.3 in Android Q(10.0) and above allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent. **CVE ID : CVE-2021-25381**	https://security.samsungmobile.com/serviceWeb.smsb, https://security.samsungmobile.com/	O-GOO-ANDR-280421/2768
N/A	13-04-2021	2.1	In injectBestLocation and handleUpdateLocation of GnssLocationProvider.java, there is a possible incorrect reporting of location data to emergency services due to improper input validation. This could lead to incorrect reporting of location data to emergency services with User	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-177561690 **CVE ID : CVE-2021-0400**		
Out-of-bounds Write	13-04-2021	4.6	In parsePrimaryFieldFirstUid Annotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174485572 **CVE ID : CVE-2021-0426**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2770
Out-of-bounds Write	13-04-2021	4.6	In parseExclusiveStateAnnotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174488848 **CVE ID : CVE-2021-0427**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	13-04-2021	2.1	In getSimSerialNumber of TelephonyManager.java, there is a possible way to read a trackable identifier due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-173421434 **CVE ID : CVE-2021-0428**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2772
Use After Free	13-04-2021	4.6	In pollOnce of ALooper.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-9 Android-10 Android-11 Android-8.1Android ID: A-175074139 **CVE ID : CVE-2021-0429**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2773
Out-of-bounds Write	13-04-2021	10	In rw_mfc_handle_read_op of rw_mfc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution via a malicious NFC packet with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11Android ID: A-178725766 **CVE ID : CVE-2021-0430**		
Out-of-bounds Read	13-04-2021	5	In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a paired device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174149901 **CVE ID : CVE-2021-0431**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2775
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-04-2021	4.4	In ClearPullerCacheIfNecessary and ForceClearPullerCache of StatsPullerManager.cpp, 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-11Android ID: A-173552790 **CVE ID : CVE-2021-0432**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2776
Improper Privilege Management	13-04-2021	5.4	In onCreate of DeviceChooserActivity.java, there is a possible way to	https://source.android.com/se	O-GOO-ANDR-280421/2777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass user consent when pairing a Bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege and pairing malicious devices with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171221090 **CVE ID : CVE-2021-0433**	curity/bulletin/2021-04-01	
Improper Initialization	13-04-2021	5	In avrc_proc_vendor_command of avrc_api.cc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174150451 **CVE ID : CVE-2021-0435**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2778
Integer Overflow or Wraparound	13-04-2021	2.1	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds read due to integer overflow. 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/2021-04-01	O-GOO-ANDR-280421/2779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496160 **CVE ID : CVE-2021-0436**		
Double Free	13-04-2021	4.6	In setPlayPolicy of DrmPlugin.cpp, there is a possible double free. This could lead to local escalation of privilege in a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176168330 **CVE ID : CVE-2021-0437**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2780
Improper Privilege Management	13-04-2021	4.4	In several functions of InputDispatcher.cpp, WindowManagerService.java, and related files, there is a possible tapjacking attack due to an incorrect FLAG_OBSCURED value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-152064592 **CVE ID : CVE-2021-0438**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2781
Out-of-bounds Write	13-04-2021	4.6	In setPowerModeWithHandle of	https://source.android.com/se	O-GOO-ANDR-280421/2782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			com_android_server_power_PowerManagerService.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174243830 **CVE ID : CVE-2021-0439**	curity/bulletin/2021-04-01	
Use After Free	13-04-2021	4.6	In updateInfo of android_hardware_input_InputApplicationHandle.cpp, there is a possible control of code flow 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-11Android ID: A-174768985 **CVE ID : CVE-2021-0442**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2783
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-04-2021	1.9	In several functions of ScreenshotHelper.java and related files, there is a possible incorrectly saved screenshot due to a race condition. This could lead to local information disclosure across user profiles with no additional execution privileges needed. User interaction is needed for	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-170474245 **CVE ID : CVE-2021-0443**		
N/A	13-04-2021	1.9	In onActivityResult of QuickContactActivity.java, there is an unnecessary return of an intent. This could lead to local information disclosure of contact data with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-178825358 **CVE ID : CVE-2021-0444**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2785
Improper Privilege Management	13-04-2021	4.6	In start of WelcomeActivity.java, there is a possible residual profile due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9Android ID: A-172322502 **CVE ID : CVE-2021-0445**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2786
Improper Privilege Management	13-04-2021	4.4	In ImportVCardActivity, there is a possible way to bypass user consent due to a tapjacking/overlay attack. This could lead to	https://source.android.com/security/bulletin/2021	O-GOO-ANDR-280421/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172252122 **CVE ID : CVE-2021-0446**	-04-01	
Improper Privilege Management	13-04-2021	4.4	In LK, there is a possible escalation of privilege due to an insecure default value. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-180427272 **CVE ID : CVE-2021-0468**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2788
Out-of-bounds Read	13-04-2021	2.1	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-176444786 **CVE ID : CVE-2021-0471**	https://source.android.com/security/bulletin/2021-04-01	O-GOO-ANDR-280421/2789
Out-of-	15-04-2021	7.2	In pb_write of pb_encode.c,	https://so	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-178754781 **CVE ID : CVE-2021-0488**	urce.android.com/security/bulletin/pixel/2021-04-01	ANDR-280421/2790
N/A	06-04-2021	2.1	An issue was discovered on LG mobile devices with Android OS 11 software. Attackers can bypass the lockscreen protection mechanism after an incoming call has been terminated. The LG ID is LVE-SMP-210002 (April 2021). **CVE ID : CVE-2021-30161**	https://lgsecurity.lge.com/	O-GOO-ANDR-280421/2791
N/A	06-04-2021	3.6	An issue was discovered on LG mobile devices with Android OS 4.4 through 11 software. Attackers can leverage ISMS services to bypass access control on specific content providers. The LG ID is LVE-SMP-210003 (April 2021). **CVE ID : CVE-2021-30162**	https://lgsecurity.lge.com/	O-GOO-ANDR-280421/2792
hp					
hp-ux					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a	https://www.ibm.com/support/pages/node/6441	O-HP-HP-U-280421/2793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	
hpe					
superdome_flex_server_firmware					
N/A	01-04-2021	4	A potential security vulnerability has been identified in HPE Superdome Flex server. A denial of service attack can be remotely exploited leaving hung connections to the BMC web interface. The monarch BMC must be rebooted to recover from this situation. Other BMC management is not impacted. HPE has made the following software update to resolve the vulnerability in HPE Superdome Flex Server: Superdome Flex Server Firmware 3.30.142 or later. **CVE ID : CVE-2021-26581**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04102en_us	O-HPE-SUPE-280421/2794
huawei					
ips_module_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-IPS_-280421/2795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
ips6000e_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-IPS6-280421/2796
ngfw_module_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-NGFW-280421/2797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
nip6000e_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-NIP6-280421/2798
nip6300_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-NIP6-280421/2799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
nip6600_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-NIP6-280421/2800
nip6800_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-NIP6-280421/2801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
secospace_usg6300_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-SECO-280421/2802
secospace_usg6500_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-SECO-280421/2803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
secospace_usg6600_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-SECO-280421/2804
usg6000e_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-	O-HUA-USG6-280421/2805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	memoryleak-en	
usg9500_firmware					
Missing Release of Memory after Effective Lifetime	08-04-2021	4	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500. **CVE ID : CVE-2021-22312**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-en	O-HUA-USG9-280421/2806
ibm					
aix					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmclo	O-IBM-AIX-280421/2807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	ud.com/vulnerabilities/197502	
i					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	O-IBM-I-280421/2808
z/os					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	O-IBM-Z/OS-280421/2809
ikuai8					
ikuaios					
N/A	06-04-2021	5	iKuaiOS 3.4.8 Build 202012291059 has an arbitrary file download vulnerability, which can be exploited by attackers to obtain sensitive information.	N/A	O-IKU-IKUA-280421/2810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28075		
intelbras					
win_300_firmware					
N/A	14-04-2021	5	The web interface on Intelbras WIN 300 and WRN 342 devices through 2021-01-04 allows remote attackers to discover credentials by reading the def_wirelesspassword line in the HTML source code. **CVE ID : CVE-2021-3017**	https://www.intelbras.com/pt-br/ajuda-download/faq/roteador-wireless-veloz-wrn-342	O-INT-WIN_-280421/2811
wrn_342_firmware					
N/A	14-04-2021	5	The web interface on Intelbras WIN 300 and WRN 342 devices through 2021-01-04 allows remote attackers to discover credentials by reading the def_wirelesspassword line in the HTML source code. **CVE ID : CVE-2021-3017**	https://www.intelbras.com/pt-br/ajuda-download/faq/roteador-wireless-veloz-wrn-342	O-INT-WRN_-280421/2812
linux					
linux_kernel					
Improper Authentication	01-04-2021	6.4	VMware Carbon Black Cloud Workload appliance 1.0.0 and 1.01 has an authentication bypass vulnerability that may allow a malicious actor with network access to the administrative interface of the VMware Carbon Black Cloud Workload appliance to obtain a valid authentication token. Successful exploitation of this issue would result in the attacker being able to	https://www.vmware.com/security/advisories/VMSA-2021-0005.html	O-LIN-LINU-280421/2813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			view and alter administrative configuration settings. **CVE ID : CVE-2021-21982**		
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	O-LIN-LINU-280421/2814
Missing Release of Resource after Effective Lifetime	02-04-2021	2.1	An issue was discovered in the Linux kernel before 5.11.3 when a webcam device exists. video_usercopy in drivers/media/v4l2-core/v4l2-ioctl.c has a memory leak for large arguments, aka CID-fb18802a338b. **CVE ID : CVE-2021-30002**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.3, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fb18802a338b36f675a388fc03d2aa504a0d0899	O-LIN-LINU-280421/2815
Improper Neutralization of Special Elements used in a Command	08-04-2021	7.2	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary	https://www.openwall.com/lists/oss-security/2021/04/0	O-LIN-LINU-280421/2816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c. **CVE ID : CVE-2021-29154**	8/1	
Improper Initialization	06-04-2021	2.1	The fix for XSA-365 includes initialization of pointers such that subsequent cleanup code wouldn't use uninitialized or stale values. This initialization went too far and may under certain conditions also overwrite pointers which are in need of cleaning up. The lack of cleanup would result in leaking persistent grants. The leak in turn would prevent fully cleaning up after a respective guest has died, leaving around zombie domains. All Linux versions having the fix for XSA-365 applied are vulnerable. XSA-365 was classified to affect versions back to at least 3.11. **CVE ID : CVE-2021-28688**	https://xenbits.xenproject.org/xsa/advisory-371.txt	O-LIN-LINU-280421/2817
NULL Pointer Dereference	07-04-2021	2.1	An issue was discovered in the Linux kernel through 5.11.11. synic_get in arch/x86/kvm/hyperv.c has a NULL pointer dereference for certain accesses to the SynIC Hyper-V context, aka CID-919f4ebc5987. **CVE ID : CVE-2021-30178**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=919f4ebc598701670e80e31573a58f1f2d2	O-LIN-LINU-280421/2818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				bf918	
microsoft					
azure_devops_server					
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability **CVE ID : CVE-2021-27067**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27067	O-MIC-AZUR-280421/2819
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2021	4.3	Azure DevOps Server Spoofing Vulnerability **CVE ID : CVE-2021-28459**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28459	O-MIC-AZUR-280421/2820
windows					
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	O-MIC-WIND-280421/2821
Out-of-bounds Write	09-04-2021	6.8	Heap buffer overflow in TabStrip in Google Chrome on Windows prior to 89.0.4389.114 allowed a remote attacker to	https://crbug.com/1175992, https://chromerelea	O-MIC-WIND-280421/2822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-21196**	ses.google blog.com/ 2021/03/ stable-channel-update-for-desktop_30.html	
Improper Privilege Management	06-04-2021	4.6	A malicious 3rd party with local access to the Windows machine where MongoDB Compass is installed can execute arbitrary software with the privileges of the user who is running MongoDB Compass. This issue affects: MongoDB Inc. MongoDB Compass 1.x version 1.3.0 on Windows and later versions; 1.x versions prior to 1.25.0 on Windows. **CVE ID : CVE-2021-20334**	https://jira.mongodb.org/browse/COMPASS-4510	O-MIC-WIND-280421/2823
Improper Authorization	15-04-2021	2.1	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Improper Authorization vulnerability in the Genuine Software Service. A low-privileged attacker could leverage this vulnerability to achieve application denial-of-service in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2021-21096**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	O-MIC-WIND-280421/2824
Out-of-bounds Write	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are	https://helpx.adobe.com/secur	O-MIC-WIND-280421/2825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected by an Out-of-bounds write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21095**	ity/products/bridge/apsb21-23.html	
Out-of-bounds Write	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21094**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	O-MIC-WIND-280421/2826
Access of Memory Location After End of Buffer	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	O-MIC-WIND-280421/2827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21093**		
Access of Memory Location After End of Buffer	15-04-2021	6.8	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21092**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	O-MIC-WIND-280421/2828
Out-of-bounds Read	15-04-2021	4.3	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-21091**	https://helpx.adobe.com/security/products/bridge/apsb21-23.html	O-MIC-WIND-280421/2829
Missing Support for Integrity Check	01-04-2021	5.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018	https://helpx.adobe.com/security/produc	O-MIC-WIND-280421/2830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to show arbitrary content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28545**	ts/acrobat/apsb21-09.html	
Missing Support for Integrity Check	01-04-2021	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are missing support for an integrity check. An unauthenticated attacker could leverage this vulnerability to modify content in a certified PDF without invalidating the certification. Exploitation of this issue requires user interaction in that a victim must open the tampered file. **CVE ID : CVE-2021-28546**	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-280421/2831
Improper Neutralization of Special Elements used in a Command ('Command	07-04-2021	4.6	The text-to-speech engine in libretro RetroArch for Windows 0.11 passes unsanitized input to PowerShell through platform_win32.c via the accessibility_speak_windows function, which allows	http://libretro.com, https://github.com/libretro/RetroArch/blob/d3dc3ee989ec6a	O-MIC-WIND-280421/2832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			attackers who have write access on filesystems that are used by RetroArch to execute code via command injection using specially a crafted file and directory names. **CVE ID : CVE-2021-28927**	4903c689907ffc47027f71f776/frontend/drivers/platform_win32.c	
Untrusted Search Path	09-04-2021	6.2	A local privilege escalation vulnerability was discovered in Erlang/OTP prior to version 23.2.3. By adding files to an existing installation's directory, a local attacker could hijack accounts of other users running Erlang programs or possibly coerce a service running with "erlsrv.exe" to execute arbitrary code as Local System. This can occur only under specific conditions on Windows with unsafe filesystem permissions. **CVE ID : CVE-2021-29221**	N/A	O-MIC-WIND-280421/2833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-04-2021	6.8	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/photoshop/apsb21-28.html	O-MIC-WIND-280421/2834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28548		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15-04-2021	6.8	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-28549**	https://helpx.adobe.com/security/products/photoshop/apsb21-28.html	O-MIC-WIND-280421/2835
Incorrect Authorization	14-04-2021	7.2	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-2021-tibco-messaging-2021-28825	O-MIC-WIND-280421/2836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition: versions 1.3.0 and below. **CVE ID : CVE-2021-28825**		
Incorrect Authorization	14-04-2021	7.2	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-2021-tibco-messaging-2021-28826	O-MIC-WIND-280421/2837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition: versions 1.3.0 and below. **CVE ID : CVE-2021-28826**		
windows_10					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/2838
N/A	13-04-2021	7.8	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-26416**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26416	O-MIC-WIND-280421/2839
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Overlay Filter Information Disclosure Vulnerability **CVE ID : CVE-2021-26417**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26417	O-MIC-WIND-280421/2840
Improper	13-04-2021	4.6	Win32k Elevation of	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-27072	280421/2841
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	6.3	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-27079**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-27079	O-MIC-WIND-280421/2842
Improper Privilege Management	13-04-2021	4.6	Windows Services and Controller App Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27086**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-27086	O-MIC-WIND-280421/2843
Improper Privilege Management	13-04-2021	4.6	Windows Event Tracing Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27088**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-27088	O-MIC-WIND-280421/2844
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution	https://po rtal.msrc. microsoft. com/en-	O-MIC-WIND-280421/2845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID : CVE-2021-27089**	US/security-guidance/advisory/CVE-2021-27089	
Improper Privilege Management	13-04-2021	4.6	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27090	O-MIC-WIND-280421/2846
N/A	13-04-2021	7.5	Azure AD Web Sign-in Security Feature Bypass Vulnerability **CVE ID : CVE-2021-27092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27092	O-MIC-WIND-280421/2847
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/2848
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-28447.	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/2849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27094	advisory/CVE-2021-27094	
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/2850
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/2851
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/2852
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/2853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28309	
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-27072. **CVE ID : CVE-2021-28310**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28310	O-MIC-WIND-280421/2854
N/A	13-04-2021	4.3	Windows Application Compatibility Cache Denial of Service Vulnerability **CVE ID : CVE-2021-28311**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28311	O-MIC-WIND-280421/2855
N/A	13-04-2021	4.3	Windows NTFS Denial of Service Vulnerability **CVE ID : CVE-2021-28312**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28312	O-MIC-WIND-280421/2856
Improper Privilege Management	13-04-2021	4.6	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28314**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28314	O-MIC-WIND-280421/2857
N/A	13-04-2021	4.6	Windows Media Video	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-28315	280421/2858
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-28316	O-MIC-WIND-280421/2859
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-28317	O-MIC-WIND-280421/2860
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://po rtal.msrc. microsoft. com/en-US/securit y-guidance/ advisory/ CVE-2021-28318	O-MIC-WIND-280421/2861
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-	https://po rtal.msrc. microsoft. com/en-	O-MIC-WIND-280421/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28439. **CVE ID : CVE-2021-28319**	US/security-guidance/advisory/CVE-2021-28319	
Improper Privilege Management	13-04-2021	4.6	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28320**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28320	O-MIC-WIND-280421/2863
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	5	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28325. **CVE ID : CVE-2021-28324**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28324	O-MIC-WIND-280421/2864
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/2865
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/2866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	advisory/CVE-2021-28327	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/2867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/2868
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/2869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/2870
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	O-MIC-WIND-280421/2871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/2872
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/2873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	US/security-guidance/advisory/CVE-2021-28335	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/2874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/2875
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/2876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/2877
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	CVE-2021-28340	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/2879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/2880
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/2882
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/2883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/2884
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/2885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	US/security-guidance/advisory/CVE-2021-28352	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/2886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/2887
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/2888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/2889
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	CVE-2021-28357	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/2892
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/2893
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28351, CVE-2021-28436. **CVE ID : CVE-2021-28347**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-28347	
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348	O-MIC-WIND-280421/2895
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/2896
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/2897
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28436. **CVE ID : CVE-2021-28351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28351	O-MIC-WIND-280421/2898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure Vulnerability **CVE ID : CVE-2021-28435**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28435	O-MIC-WIND-280421/2899
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28351. **CVE ID : CVE-2021-28436**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28436	O-MIC-WIND-280421/2900
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/2901
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28443. **CVE ID : CVE-2021-28438**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28438	O-MIC-WIND-280421/2902
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is	https://portal.msrc.microsoft.	O-MIC-WIND-280421/2903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	com/en-US/security-guidance/advisory/CVE-2021-28439	
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/2904
N/A	13-04-2021	2.1	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2021-28441**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28441	O-MIC-WIND-280421/2905
N/A	13-04-2021	4	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2021-28442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28442	O-MIC-WIND-280421/2906
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/2907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28443	guidance/ advisory/ CVE-2021-28443	
N/A	13-04-2021	4	Windows Hyper-V Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28444**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28444	O-MIC-WIND-280421/2908
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/2909
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-280421/2910
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/2911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28447	
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322. **CVE ID : CVE-2021-28313**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28313	O-MIC-WIND-280421/2912
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321	O-MIC-WIND-280421/2913
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322	O-MIC-WIND-280421/2914
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-280421/2915
N/A	13-04-2021	4.3	Windows AppX	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deployment Server Denial of Service Vulnerability **CVE ID : CVE-2021-28326**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28326	280421/2916
windows_7					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/2917
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/2918
Improper Privilege Management	13-04-2021	4.6	RPC Endpoint Mapper Service Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27091	O-MIC-WIND-280421/2919
Exposure of Sensitive	13-04-2021	2.1	Windows Kernel Information Disclosure	https://portal.msrc.	O-MIC-WIND-280421/2920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/2921
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/2922
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/2923
Exposure of Sensitive Information to an Unauthorized	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/2924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Actor			27093. **CVE ID : CVE-2021-28309**	y-guidance/advisory/CVE-2021-28309	
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/2925
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	O-MIC-WIND-280421/2926
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/2927
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-28318	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327	O-MIC-WIND-280421/2929
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/2930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/2931
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/2932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**	28331	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/2933
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code	https://portal.msrc.	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	280421/2934
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28335	O-MIC-WIND-280421/2936
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/2937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/2938
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/2939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**	guidance/advisory/CVE-2021-28338	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/2940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28339		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340	O-MIC-WIND-280421/2941
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/2942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/2943
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/2944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**	28343	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/2945
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/2946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**	com/en-US/security-guidance/advisory/CVE-2021-28345	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/2947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28352	O-MIC-WIND-280421/2948
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/2949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/2950
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/2951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**	advisory/CVE-2021-28355	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/2952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357	O-MIC-WIND-280421/2953
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/2954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/2955
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/2956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348	O-MIC-WIND-280421/2957
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/2958
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/2959
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/2960
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is	https://portal.msrc.microsoft.	O-MIC-WIND-280421/2961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	com/en-US/security-guidance/advisory/CVE-2021-28439	
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/2962
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-280421/2963
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/2964
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/2965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-28446	
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-280421/2966
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-280421/2967
windows_8.1					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/2968
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/2969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-27072	
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/2970
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/2971
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-28447. **CVE ID : CVE-2021-27094**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27094	O-MIC-WIND-280421/2972
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/2973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				27095	
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/2974
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/2975
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28309	O-MIC-WIND-280421/2976
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/2977
N/A	13-04-2021	2.1	Windows WLAN	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	280421/2978
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/2979
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28318	O-MIC-WIND-280421/2980
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/2981
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/2982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	US/security-guidance/advisory/CVE-2021-28327	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/2984
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/2985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/2986
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**	CVE-2021-28333	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/2988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28335	O-MIC-WIND-280421/2989
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/2990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/2991
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/2992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/2993
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	US/security-guidance/advisory/CVE-2021-28340	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/2995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/2996
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/2997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/2998
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/2999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**	CVE-2021-28345	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/3000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28352	O-MIC-WIND-280421/3001
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/3002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/3003
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3005
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	US/security-guidance/advisory/CVE-2021-28357	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/3007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/3008
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3009
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	US/security-guidance/advisory/CVE-2021-28348	
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/3011
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/3012
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure Vulnerability **CVE ID : CVE-2021-28435**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28435	O-MIC-WIND-280421/3013
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-28437	
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439	O-MIC-WIND-280421/3015
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3016
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-280421/3017
N/A	13-04-2021	4	Windows Hyper-V Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28444**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28444	
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/3019
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-280421/3020
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-280421/3021
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-280421/3022
windows_rt_8.1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/3023
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27072	O-MIC-WIND-280421/3024
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/3025
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/3026
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability This CVE ID is unique from CVE-2021-28447. **CVE ID : CVE-2021-27094**	com/en-US/security-guidance/advisory/CVE-2021-27094	
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/3028
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/3029
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/3030
Exposure of Sensitive Information to an Unauthorized	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Actor			**CVE ID : CVE-2021-28309**	guidance/ advisory/ CVE-2021-28309	
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/3032
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	O-MIC-WIND-280421/3033
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/3034
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28318	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/3036
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327	O-MIC-WIND-280421/3037
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**	advisory/CVE-2021-28329	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/3039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/3040
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/3041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	O-MIC-WIND-280421/3042
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28335	O-MIC-WIND-280421/3044
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**	US/security-guidance/advisory/CVE-2021-28336	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/3046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/3047
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/3048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340	O-MIC-WIND-280421/3049
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	CVE-2021-28341	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/3051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/3052
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/3053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/3054
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/3055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28352	O-MIC-WIND-280421/3056
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**	US/security-guidance/advisory/CVE-2021-28353	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/3058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3059
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357	O-MIC-WIND-280421/3061
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	CVE-2021-28358	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/3063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3064
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348	O-MIC-WIND-280421/3065
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/3066
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/3067
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID : CVE-2021-28435**	com/en-US/security-guidance/advisory/CVE-2021-28435	
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/3069
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439	O-MIC-WIND-280421/3070
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3071
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28443	guidance/advisory/CVE-2021-28443	
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/3073
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-280421/3074
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-280421/3075
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28323	
windows_server_2008					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/3077
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/3078
Improper Privilege Management	13-04-2021	4.6	RPC Endpoint Mapper Service Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27091**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27091	O-MIC-WIND-280421/3079
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/3080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/3081
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/3082
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/3083
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28309	O-MIC-WIND-280421/3084
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	com/en-US/security-guidance/advisory/CVE-2021-28315	
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	O-MIC-WIND-280421/3086
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/3087
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28318	O-MIC-WIND-280421/3088
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	guidance/advisory/CVE-2021-28327	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/3090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28329		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/3091
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/3092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/3093
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**	28333	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/3095
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	com/en-US/security-guidance/advisory/CVE-2021-28335	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/3097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/3098
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/3099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/3100
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	advisory/CVE-2021-28340	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/3102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/3103
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/3104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/3105
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/3106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/3107
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	US/security-guidance/advisory/CVE-2021-28352	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/3109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/3110
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3112
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	CVE-2021-28357	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/3114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/3115
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3116
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-28348	
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/3118
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/3119
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/3120
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439	O-MIC-WIND-280421/3121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3122
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-280421/3123
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/3124
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-280421/3125
Exposure of Sensitive Information	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			CVE-2021-28328. **CVE ID : CVE-2021-28323**	com/en-US/security-guidance/advisory/CVE-2021-28323	
windows_server_2012					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/3127
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27072	O-MIC-WIND-280421/3128
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/3129
Improper Privilege Management	13-04-2021	4.6	RPC Endpoint Mapper Service Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27091**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				US/security-guidance/advisory/CVE-2021-27091	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/3131
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-28447. **CVE ID : CVE-2021-27094**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27094	O-MIC-WIND-280421/3132
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/3133
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-27096	
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/3135
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28309	O-MIC-WIND-280421/3136
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/3137
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28316	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/3139
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28318	O-MIC-WIND-280421/3140
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/3141
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327	O-MIC-WIND-280421/3142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/3143
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	y-guidance/advisory/CVE-2021-28330	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/3145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28434. **CVE ID : CVE-2021-28331**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/3146
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	O-MIC-WIND-280421/3147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/3148
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	28335	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/3150
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code	https://portal.msrc.	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	280421/3151
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/3152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/3153
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340	O-MIC-WIND-280421/3154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/3155
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	guidance/advisory/CVE-2021-28342	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/3157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28343		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/3158
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/3159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/3160
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	28352	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/3162
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	com/en-US/security-guidance/advisory/CVE-2021-28354	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3165
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357	O-MIC-WIND-280421/3166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/3167
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	advisory/CVE-2021-28434	
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3169
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348	O-MIC-WIND-280421/3170
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	y-guidance/advisory/CVE-2021-28349	
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/3172
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure Vulnerability **CVE ID : CVE-2021-28435**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28435	O-MIC-WIND-280421/3173
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/3174
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-28439	
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3176
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-280421/3177
N/A	13-04-2021	4	Windows Hyper-V Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28444**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28444	O-MIC-WIND-280421/3178
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-280421/3180
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-280421/3181
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-280421/3182
windows_server_2016					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/3183
N/A	13-04-2021	7.8	Windows Hyper-V Denial	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Service Vulnerability **CVE ID : CVE-2021-26416**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26416	280421/3184
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Overlay Filter Information Disclosure Vulnerability **CVE ID : CVE-2021-26417**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26417	O-MIC-WIND-280421/3185
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27072	O-MIC-WIND-280421/3186
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	6.3	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-27079**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27079	O-MIC-WIND-280421/3187
Improper Privilege Management	13-04-2021	4.6	Windows Services and Controller App Elevation of Privilege Vulnerability	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27086	US/security-guidance/advisory/CVE-2021-27086	
Improper Privilege Management	13-04-2021	4.6	Windows Event Tracing Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27088	O-MIC-WIND-280421/3189
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/3190
Improper Privilege Management	13-04-2021	4.6	Windows Secure Kernel Mode Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27090**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27090	O-MIC-WIND-280421/3191
N/A	13-04-2021	7.5	Azure AD Web Sign-in Security Feature Bypass Vulnerability **CVE ID : CVE-2021-27092**	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-27092	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/3193
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-28447. **CVE ID : CVE-2021-27094**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27094	O-MIC-WIND-280421/3194
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/3195
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				27096	
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/3197
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28309	O-MIC-WIND-280421/3198
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-27072. **CVE ID : CVE-2021-28310**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28310	O-MIC-WIND-280421/3199
N/A	13-04-2021	4.3	Windows Application Compatibility Cache Denial of Service Vulnerability **CVE ID : CVE-2021-28311**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28311	O-MIC-WIND-280421/3200
N/A	13-04-2021	4.3	Windows NTFS Denial of	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability **CVE ID : CVE-2021-28312**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28312	280421/3201
Improper Privilege Management	13-04-2021	4.6	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28314**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28314	O-MIC-WIND-280421/3202
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/3203
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	O-MIC-WIND-280421/3204
Exposure of Sensitive Information to an	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			**CVE ID : CVE-2021-28317**	US/security-guidance/advisory/CVE-2021-28317	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28318	O-MIC-WIND-280421/3206
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28439. **CVE ID : CVE-2021-28319**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28319	O-MIC-WIND-280421/3207
Improper Privilege Management	13-04-2021	4.6	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28320**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28320	O-MIC-WIND-280421/3208
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	5	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28325. **CVE ID : CVE-2021-28324**	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				advisory/CVE-2021-28324	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/3210
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327	O-MIC-WIND-280421/3211
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**	y-guidance/advisory/CVE-2021-28329	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330	O-MIC-WIND-280421/3213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28434. **CVE ID : CVE-2021-28330**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28331**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/3214
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/3215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	O-MIC-WIND-280421/3216
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	28334	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28335	O-MIC-WIND-280421/3218
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code	https://portal.msrc.	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	280421/3219
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	O-MIC-WIND-280421/3220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/3221
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/3222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340	O-MIC-WIND-280421/3223
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	guidance/advisory/CVE-2021-28341	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342	O-MIC-WIND-280421/3225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28342		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28343**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/3226
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/3227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/3228
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	28346	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28352	O-MIC-WIND-280421/3230
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**	com/en-US/security-guidance/advisory/CVE-2021-28353	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354	O-MIC-WIND-280421/3232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3233
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357	O-MIC-WIND-280421/3235
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	advisory/CVE-2021-28358	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434	O-MIC-WIND-280421/3237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3238
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28351, CVE-2021-28436. **CVE ID : CVE-2021-28347**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28347	O-MIC-WIND-280421/3239
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348	O-MIC-WIND-280421/3240
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/3241
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	com/en-US/security-guidance/advisory/CVE-2021-28350	
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28436. **CVE ID : CVE-2021-28351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28351	O-MIC-WIND-280421/3243
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure Vulnerability **CVE ID : CVE-2021-28435**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28435	O-MIC-WIND-280421/3244
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28351. **CVE ID : CVE-2021-28436**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28436	O-MIC-WIND-280421/3245
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-28437	
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28443. **CVE ID : CVE-2021-28438**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28438	O-MIC-WIND-280421/3247
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439	O-MIC-WIND-280421/3248
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3249
N/A	13-04-2021	2.1	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2021-28441**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28441	
N/A	13-04-2021	4	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2021-28442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28442	O-MIC-WIND-280421/3251
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-280421/3252
N/A	13-04-2021	4	Windows Hyper-V Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28444**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28444	O-MIC-WIND-280421/3253
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-280421/3254
N/A	13-04-2021	2.1	Windows Portmapping	https://po	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	rtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	280421/3255
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-280421/3256
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-2021-28322. **CVE ID : CVE-2021-28313**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28313	O-MIC-WIND-280421/3257
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321	O-MIC-WIND-280421/3258
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-280421/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	US/security-guidance/advisory/CVE-2021-28322	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-280421/3260
N/A	13-04-2021	4.3	Windows AppX Deployment Server Denial of Service Vulnerability **CVE ID : CVE-2021-28326**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28326	O-MIC-WIND-280421/3261
windows_server_2019					
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28440. **CVE ID : CVE-2021-26415**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415	O-MIC-WIND-280421/3262
N/A	13-04-2021	7.8	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2021-26416**	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				y-guidance/advisory/CVE-2021-26416	
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Overlay Filter Information Disclosure Vulnerability **CVE ID : CVE-2021-26417**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26417	O-MIC-WIND-280421/3264
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28310. **CVE ID : CVE-2021-27072**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27072	O-MIC-WIND-280421/3265
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	6.3	Windows Media Photo Codec Information Disclosure Vulnerability **CVE ID : CVE-2021-27079**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27079	O-MIC-WIND-280421/3266
Improper Privilege Management	13-04-2021	4.6	Windows Services and Controller App Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27086**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-27086	
Improper Privilege Management	13-04-2021	4.6	Windows Event Tracing Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27088**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27088	O-MIC-WIND-280421/3268
N/A	13-04-2021	6.8	Microsoft Internet Messaging API Remote Code Execution Vulnerability **CVE ID : CVE-2021-27089**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089	O-MIC-WIND-280421/3269
N/A	13-04-2021	7.5	Azure AD Web Sign-in Security Feature Bypass Vulnerability **CVE ID : CVE-2021-27092**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27092	O-MIC-WIND-280421/3270
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28309. **CVE ID : CVE-2021-27093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093	O-MIC-WIND-280421/3271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-28447. **CVE ID : CVE-2021-27094**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27094	O-MIC-WIND-280421/3272
N/A	13-04-2021	6.8	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28315. **CVE ID : CVE-2021-27095**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095	O-MIC-WIND-280421/3273
Improper Privilege Management	13-04-2021	4.6	NTFS Elevation of Privilege Vulnerability **CVE ID : CVE-2021-27096**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096	O-MIC-WIND-280421/3274
N/A	13-04-2021	2.1	Windows Installer Spoofing Vulnerability **CVE ID : CVE-2021-26413**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413	O-MIC-WIND-280421/3275
Exposure of Sensitive Information	13-04-2021	2.1	Windows Kernel Information Disclosure Vulnerability This CVE ID is	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			unique from CVE-2021-27093. **CVE ID : CVE-2021-28309**	com/en-US/security-guidance/advisory/CVE-2021-28309	
Improper Privilege Management	13-04-2021	4.6	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-27072. **CVE ID : CVE-2021-28310**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28310	O-MIC-WIND-280421/3277
N/A	13-04-2021	4.3	Windows Application Compatibility Cache Denial of Service Vulnerability **CVE ID : CVE-2021-28311**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28311	O-MIC-WIND-280421/3278
N/A	13-04-2021	4.3	Windows NTFS Denial of Service Vulnerability **CVE ID : CVE-2021-28312**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28312	O-MIC-WIND-280421/3279
Improper Privilege Management	13-04-2021	4.6	Windows Hyper-V Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28314**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				guidance/advisory/CVE-2021-28314	
N/A	13-04-2021	4.6	Windows Media Video Decoder Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-27095. **CVE ID : CVE-2021-28315**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315	O-MIC-WIND-280421/3281
N/A	13-04-2021	2.1	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability **CVE ID : CVE-2021-28316**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316	O-MIC-WIND-280421/3282
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Microsoft Windows Codecs Library Information Disclosure Vulnerability **CVE ID : CVE-2021-28317**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317	O-MIC-WIND-280421/3283
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	2.1	Windows GDI+ Information Disclosure Vulnerability **CVE ID : CVE-2021-28318**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28318	
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28439. **CVE ID : CVE-2021-28319**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28319	O-MIC-WIND-280421/3285
Improper Privilege Management	13-04-2021	4.6	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability **CVE ID : CVE-2021-28320**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28320	O-MIC-WIND-280421/3286
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324. **CVE ID : CVE-2021-28325**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325	O-MIC-WIND-280421/3287
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327	O-MIC-WIND-280421/3288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28327**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28329**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329	O-MIC-WIND-280421/3289
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28329, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28330**	y-guidance/advisory/CVE-2021-28330	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331	O-MIC-WIND-280421/3291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28434. **CVE ID : CVE-2021-28331**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28332**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332	O-MIC-WIND-280421/3292
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333	O-MIC-WIND-280421/3293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28333**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28334**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334	O-MIC-WIND-280421/3294
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28334, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28335**	28335	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28336**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336	O-MIC-WIND-280421/3296
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code	https://portal.msrc.	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28337**	microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337	280421/3297
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338	O-MIC-WIND-280421/3298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28338**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339	O-MIC-WIND-280421/3299
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340	O-MIC-WIND-280421/3300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28340**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28341**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341	O-MIC-WIND-280421/3301
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-280421/3302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28342**	guidance/advisory/CVE-2021-28342	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343	O-MIC-WIND-280421/3303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-28343		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344	O-MIC-WIND-280421/3304
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345	O-MIC-WIND-280421/3305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28345**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28346**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346	O-MIC-WIND-280421/3306
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-280421/3307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28352**	28352	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28353**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353	O-MIC-WIND-280421/3308
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://portal.msrc.microsoft.	O-MIC-WIND-280421/3309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28354**	com/en-US/security-guidance/advisory/CVE-2021-28354	
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355	O-MIC-WIND-280421/3310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28356, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28355**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28357, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28356**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356	O-MIC-WIND-280421/3311
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357	O-MIC-WIND-280421/3312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28358, CVE-2021-28434. **CVE ID : CVE-2021-28357**		
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331, CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28434. **CVE ID : CVE-2021-28358**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358	O-MIC-WIND-280421/3313
N/A	13-04-2021	6.5	Remote Procedure Call Runtime Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28327, CVE-2021-28329, CVE-2021-28330, CVE-2021-28331,	https://portal.msrc.microsoft.com/en-US/security-guidance/	O-MIC-WIND-280421/3314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2021-28332, CVE-2021-28333, CVE-2021-28334, CVE-2021-28335, CVE-2021-28336, CVE-2021-28337, CVE-2021-28338, CVE-2021-28339, CVE-2021-28340, CVE-2021-28341, CVE-2021-28342, CVE-2021-28343, CVE-2021-28344, CVE-2021-28345, CVE-2021-28346, CVE-2021-28352, CVE-2021-28353, CVE-2021-28354, CVE-2021-28355, CVE-2021-28356, CVE-2021-28357, CVE-2021-28358. **CVE ID : CVE-2021-28434**	advisory/CVE-2021-28434	
N/A	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28323. **CVE ID : CVE-2021-28328**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328	O-MIC-WIND-280421/3315
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28351, CVE-2021-28436. **CVE ID : CVE-2021-28347**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28347	O-MIC-WIND-280421/3316
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-	https://portal.msrc.microsoft.com/en-US/securit	O-MIC-WIND-280421/3317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			28349, CVE-2021-28350. **CVE ID : CVE-2021-28348**	y-guidance/advisory/CVE-2021-28348	
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28350. **CVE ID : CVE-2021-28349**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349	O-MIC-WIND-280421/3318
N/A	13-04-2021	4.6	Windows GDI+ Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-28348, CVE-2021-28349. **CVE ID : CVE-2021-28350**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350	O-MIC-WIND-280421/3319
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28436. **CVE ID : CVE-2021-28351**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28351	O-MIC-WIND-280421/3320
N/A	13-04-2021	2.1	Windows Event Tracing Information Disclosure Vulnerability **CVE ID : CVE-2021-28435**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/	O-MIC-WIND-280421/3321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				CVE-2021-28435	
Improper Privilege Management	13-04-2021	4.6	Windows Speech Runtime Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28347, CVE-2021-28351. **CVE ID : CVE-2021-28436**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28436	O-MIC-WIND-280421/3322
N/A	13-04-2021	2.1	Windows Installer Information Disclosure Vulnerability **CVE ID : CVE-2021-28437**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437	O-MIC-WIND-280421/3323
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28443. **CVE ID : CVE-2021-28438**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28438	O-MIC-WIND-280421/3324
N/A	13-04-2021	5	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28319. **CVE ID : CVE-2021-28439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439	O-MIC-WIND-280421/3325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	13-04-2021	4.6	Windows Installer Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26415. **CVE ID : CVE-2021-28440**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440	O-MIC-WIND-280421/3326
N/A	13-04-2021	2.1	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2021-28441**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28441	O-MIC-WIND-280421/3327
N/A	13-04-2021	4	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2021-28442**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28442	O-MIC-WIND-290421/3328
N/A	13-04-2021	2.1	Windows Console Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-28438. **CVE ID : CVE-2021-28443**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443	O-MIC-WIND-290421/3329
N/A	13-04-2021	4	Windows Hyper-V Security Feature Bypass	https://portal.msrc.microsoft.	O-MIC-WIND-290421/3330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID : CVE-2021-28444**	com/en-US/security-guidance/advisory/CVE-2021-28444	
N/A	13-04-2021	6.5	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2021-28445**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445	O-MIC-WIND-290421/3331
N/A	13-04-2021	2.1	Windows Portmapping Information Disclosure Vulnerability **CVE ID : CVE-2021-28446**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446	O-MIC-WIND-290421/3332
N/A	13-04-2021	2.1	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability This CVE ID is unique from CVE-2021-27094. **CVE ID : CVE-2021-28447**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447	O-MIC-WIND-290421/3333
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28321, CVE-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-290421/3334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-28322. **CVE ID : CVE-2021-28313**	guidance/ advisory/ CVE-2021-28313	
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28322. **CVE ID : CVE-2021-28321**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321	O-MIC-WIND-290421/3335
Improper Privilege Management	13-04-2021	4.6	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-28313, CVE-2021-28321. **CVE ID : CVE-2021-28322**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322	O-MIC-WIND-290421/3336
Exposure of Sensitive Information to an Unauthorized Actor	13-04-2021	4	Windows DNS Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28328. **CVE ID : CVE-2021-28323**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323	O-MIC-WIND-290421/3337
N/A	13-04-2021	4.3	Windows AppX Deployment Server Denial of Service Vulnerability **CVE ID : CVE-2021-28326**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-	O-MIC-WIND-290421/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				28326	
motorola					
mh702x_firmware					
Improper Certificate Validation	13-04-2021	7.5	The Motorola MH702x devices, prior to version 2.0.0.301, do not properly verify the server certificate during communication with the support server which could lead to the communication channel being accessible by an attacker. **CVE ID : CVE-2021-3460**	https://motorolamentor.zendesk.com/hc/en-us/articles/1260804087249	O-MOT-MH70-290421/3339
multilaser					
ac1200_firmware					
Cross-Site Request Forgery (CSRF)	14-04-2021	6.8	Multilaser Router AC1200 V02.03.01.45_pt contains a cross-site request forgery (CSRF) vulnerability. An attacker can enable remote access, change passwords, and perform other actions through misconfigured requests, entries, and headers. **CVE ID : CVE-2021-31152**	N/A	O-MUL-AC12-290421/3340
nokia					
g-120w-f_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2021	3.5	An issue was discovered on Nokia G-120W-F 3FE46606AGAB91 devices. There is Stored XSS in the administrative interface via urlfilter.cgi?add url_address. **CVE ID : CVE-2021-30003**	N/A	O-NOK-G-12-290421/3341
oracle					
solaris					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	08-04-2021	4	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502. **CVE ID : CVE-2021-20480**	https://www.ibm.com/support/pages/node/6441063, https://exchange.xforce.ibmcloud.com/vulnerabilities/197502	O-ORA-SOLA-290421/3342
qualcomm					
aqt1000_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-AQT1-290421/3343
pm8005_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-PM80-290421/3344
pm855_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-PM85-290421/3345
pm855p_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-PM85-290421/3346
pm8998_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-PM89-290421/3347
pmi8998_firmware					
Improper Input	07-04-2021	7.2	Memory corruption due to improper input validation	https://www.qualco	O-QUA-PMI8-290421/3348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	mm.com/company/product-security/bulletins/april-2021-bulletin	
qat3550_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QAT3-290421/3349
qca1062_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA1-290421/3350
qca1064_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in	https://www.qualcomm.com/company/p	O-QUA-QCA1-290421/3351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	roduct-security/bulletins/april-2021-bulletin	
qca2066_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA2-290421/3352
qca6164_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3353
qca6174_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/b	O-QUA-QCA6-290421/3354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	ulletins/april-2021-bulletin	
qca6174a_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3355
qca6310_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3356
qca6335_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/april-2021-	O-QUA-QCA6-290421/3357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	bulletin	
qca6391_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3358
qca6420_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3359
qca6430_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1892**		
qca6595au_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA6-290421/3361
qca9377_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCA9-290421/3362
qcn7605_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCN7-290421/3363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1892		
qcn7606_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QCN7-290421/3364
qet4100_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QET4-290421/3365
qfe2081fc_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QFE2-290421/3366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qfe2082fc_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QFE2-290421/3367
qfe3100_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QFE3-290421/3368
qfe3440fc_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QFE3-290421/3369
qfe4455fc_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QFE4-290421/3370
qln1035bd_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-QLN1-290421/3371
sd835_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SD83-290421/3372
sd845_firmware					
Improper Input	07-04-2021	7.2	Memory corruption due to improper input validation	https://www.qualco	O-QUA-SD84-290421/3373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	mm.com/company/product-security/bulletins/april-2021-bulletin	
sd850_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SD85-290421/3374
sd8c_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SD8C-290421/3375
sd8cx_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in	https://www.qualcomm.com/company/p	O-QUA-SD8C-290421/3376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	roduct-security/bulletins/april-2021-bulletin	
sdr8150_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SDR8-290421/3377
smb1350_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SMB1-290421/3378
smb1351_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/b	O-QUA-SMB1-290421/3379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	ulletins/april-2021-bulletin	
smb1380_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SMB1-290421/3380
smb1381_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SMB1-290421/3381
smb1390_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/april-2021-	O-QUA-SMB1-290421/3382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	bulletin	
smb2351_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-SMB2-290421/3383
wcd9335_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCD9-290421/3384
wcd9340_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCD9-290421/3385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1892**		
wcd9341_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCD9-290421/3386
wcn3990_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN3-290421/3387
wcn3998_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN3-290421/3388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1892		
wcn6850_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN6-290421/3389
wcn6851_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN6-290421/3390
wcn6855_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN6-290421/3391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcn6856_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WCN6-290421/3392
wgr7640_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WGR7-290421/3393
wsa8810_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WSA8-290421/3394
wsa8815_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WSA8-290421/3395
wtr5975_firmware					
Improper Input Validation	07-04-2021	7.2	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1892**	https://www.qualcomm.com/company/product-security/bulletins/april-2021-bulletin	O-QUA-WTR5-290421/3396
redhat					
enterprise_linux					
Improper Locking	01-04-2021	7.1	A deadlock vulnerability was found in 'github.com/containers/storage' in versions before 1.28.1. When a container image is processed, each layer is unpacked using `tar`. If one of those layers is not a valid `tar` archive this causes an error leading to an unexpected situation where the code indefinitely waits for the tar unpacked stream, which never finishes. An attacker could	https://bugzilla.redhat.com/show_bug.cgi?id=1939485	O-RED-ENTE-290421/3397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use this vulnerability to craft a malicious image, which when downloaded and stored by an application using containers/storage, would then cause a deadlock leading to a Denial of Service (DoS). **CVE ID : CVE-2021-20291**		
Use of a Broken or Risky Cryptographic Algorithm	05-04-2021	6.8	A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2021-20305**	https://bugzilla.redhat.com/show_bug.cgi?id=1942533	O-RED-ENTE-290421/3398
Generation of Error Message Containing Sensitive Information	01-04-2021	3.5	An information leak was discovered in postgresql in versions before 13.2, before 12.6 and before 11.11. A user having UPDATE permission but not SELECT permission to a particular column could craft queries which, under some circumstances, might disclose values from that column in error messages.	N/A	O-RED-ENTE-290421/3399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could use this flaw to obtain information stored in a column they are allowed to write but not read. **CVE ID : CVE-2021-3393**		
N/A	08-04-2021	4.3	A flaw was found in dnsmasq in versions before 2.85. When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this vulnerability is to data integrity. **CVE ID : CVE-2021-3448**	https://bugzilla.redhat.com/show_bug.cgi?id=1939368	O-RED-ENTE-290421/3400
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2021	6.4	A flaw was found in Exiv2 in versions before and including 0.27.4-RC1. Improper input validation of the rawData.size property in Jp2Image::readMetadata() in jp2image.cpp can lead to a heap-based buffer overflow via a crafted JPG image containing malicious EXIF data. **CVE ID : CVE-2021-3482**	https://bugzilla.redhat.com/show_bug.cgi?id=1946314	O-RED-ENTE-290421/3401
Improper Input	15-04-2021	7.1	There's a flaw in the BFD library of binutils in	https://bugzilla.redh	O-RED-ENTE-290421/3402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			versions before 2.36. An attacker who supplies a crafted file to an application linked with BFD, and using the DWARF functionality, could cause an impact to system availability by way of excessive memory consumption. **CVE ID : CVE-2021-3487**	at.com/show_bug.cgi?id=1947111	
riot-os					
riot					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	7.5	RIOT-OS 2020.01 contains a buffer overflow vulnerability in /sys/net/gnrc/routing/rpl/gnrc_rpl_control_messages.c. **CVE ID : CVE-2021-27357**	N/A	O-RIO-RIOT-290421/3403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	7.5	RIOT-OS 2021.01 contains a buffer overflow vulnerability in sys/net/gnrc/routing/rpl/gnrc_rpl_validation.c through the gnrc_rpl_validation_options() function. **CVE ID : CVE-2021-27697**	N/A	O-RIO-RIOT-290421/3404
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	7.5	RIOT-OS 2021.01 contains a buffer overflow vulnerability in /sys/net/gnrc/routing/rpl/gnrc_rpl_control_messages.c through the _parse_options() function. **CVE ID : CVE-2021-27698**	N/A	O-RIO-RIOT-290421/3405
serenityos					
serenity					
Buffer Copy	06-04-2021	5	SerenityOS Unspecified is	https://git	O-SER-SERE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			affected by: Buffer Overflow. The impact is: obtain sensitive information (context-dependent). The component is: /Userland/Libraries/LibCrypto/ASN1/DER.h Crypto::der_decode_sequence() function. The attack vector is: Parsing RSA Key ASN.1. **CVE ID : CVE-2021-27343**	hub.com/SerenityOS/serenity/commit/48fbf6a88d4822a1e5470cf08f29464511bd72c1	290421/3406
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	6.8	SerenityOS fixed as of c9f25bca048443e317f1994ba9b106f2386688c3 contains a buffer overflow vulnerability in LibTextCode through opening a crafted file. **CVE ID : CVE-2021-28874**	N/A	O-SER-SERE-290421/3407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-04-2021	6.4	SerenityOS 2021-03-27 contains a buffer overflow vulnerability in the EndOfCentralDirectory::read() function. **CVE ID : CVE-2021-30045**	https://github.com/SerenityOS/serenity/commit/4317db7498eaa5a37068052bb0310fbc6a5f78e4	O-SER-SERE-290421/3408
skyworthdigital					
rn510_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2021	3.5	Skyworth Digital Technology RN510 V.3.1.0.4 is affected by an incorrect access control vulnerability in/cgi-bin/test_version.asp. If Wi-Fi is connected but an unauthenticated user visits a URL, the SSID password	N/A	O-SKY-RN51-290421/3409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and web UI password may be disclosed. **CVE ID : CVE-2021-25326**		
Cross-Site Request Forgery (CSRF)	09-04-2021	4.3	Skyworth Digital Technology RN510 V.3.1.0.4 contains a cross-site request forgery (CSRF) vulnerability in /cgi-bin/net-routeadd.asp and /cgi-bin/sec-urlfilter.asp. Missing CSRF protection in devices can lead to XSRF, as the above pages are vulnerable to cross-site scripting (XSS). **CVE ID : CVE-2021-25327**	N/A	O-SKY-RN51-290421/3410
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2021	6.5	Skyworth Digital Technology RN510 V.3.1.0.4 RN510 V.3.1.0.4 contains a buffer overflow vulnerability in /cgi-bin/app-staticIP.asp. An authenticated attacker can send a specially crafted request to endpoint which can lead to a denial of service (DoS) or possible code execution on the device. **CVE ID : CVE-2021-25328**	N/A	O-SKY-RN51-290421/3411
suse					
linux_enterprise_server					
Insecure Temporary File	14-04-2021	2.1	A Insecure Temporary File vulnerability in s390-tools of SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-SP2 allows local attackers to prevent VM live migrations This issue affects: SUSE Linux Enterprise Server	https://bugzilla.suse.com/show_bug.cgi?id=1182777	O-SUS-LINU-290421/3412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12-SP5 s390-tools versions prior to 2.1.0-18.29.1. SUSE Linux Enterprise Server 15-SP2 s390-tools versions prior to 2.11.0-9.20.1. **CVE ID : CVE-2021-25316**		
tenda					
g1_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"qosIndex "request. This occurs because the "formQOSRuleDel" function directly passes the parameter "qosIndex" to strcpy without limit. **CVE ID : CVE-2021-27705**	N/A	O-TEN-G1_F-290421/3413
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware version V15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"IPMacBindIndex "request. This occurs because the "formIPMacBindDel" function directly passes the parameter "IPMacBindIndex" to strcpy without limit. **CVE ID : CVE-2021-27706**	N/A	O-TEN-G1_F-290421/3414
Buffer Copy without Checking Size	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware	N/A	O-TEN-G1_F-290421/3415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"portMappingIndex "request. This occurs because the "formDelPortMapping" function directly passes the parameter "portMappingIndex" to strcpy without limit. **CVE ID : CVE-2021-27707**		
g3_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"qosIndex "request. This occurs because the "formQOSRuleDel" function directly passes the parameter "qosIndex" to strcpy without limit. **CVE ID : CVE-2021-27705**	N/A	O-TEN-G3_F-290421/3416
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware version V15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"IPMacBindIndex "request. This occurs because the "formIPMacBindDel" function directly passes the parameter "IPMacBindIndex" to strcpy	N/A	O-TEN-G3_F-290421/3417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without limit. **CVE ID : CVE-2021-27706**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.5	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"portMappingIndex "request. This occurs because the "formDelPortMapping" function directly passes the parameter "portMappingIndex" to strcpy without limit. **CVE ID : CVE-2021-27707**	N/A	O-TEN-G3_F-290421/3418
terra-master					
f2-210_firmware					
Incorrect Authorization	03-04-2021	7.5	TerraMaster F2-210 devices through 2021-04-03 use UPnP to make the admin web server accessible over the Internet on TCP port 8181, which is arguably inconsistent with the "It is only available on the local network" documentation. NOTE: manually editing /etc/upnp.json provides a partial but undocumented workaround. **CVE ID : CVE-2021-30127**	N/A	O-TER-F2-2-290421/3419
totolink					
a720r_firmware					
Improper Neutralization of Special Elements	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102,	N/A	O-TOT-A720-290421/3420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS. **CVE ID : CVE-2021-27708**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "ip" parameter is directly passed to the attacker, allowing them to control the "ip" field to attack the OS. **CVE ID : CVE-2021-27710**	N/A	O-TOT-A720-290421/3421
x5000r_firmware					
Improper Neutralizatio	14-04-2021	10	Command Injection in TOTOLINK X5000R router	N/A	O-TOT-X500-290421/3422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS. **CVE ID : CVE-2021-27708**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-04-2021	10	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "ip" parameter is directly passed to the attacker, allowing them to control the "ip" field to attack the OS. **CVE ID : CVE-2021-27710**	N/A	O-TOT-X500-290421/3423
tp-link					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tl-wr2041+_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	14-04-2021	7.8	Buffer Overflow in TP-Link WR2041 v1 firmware for the TL-WR2041+ router allows remote attackers to cause a Denial-of-Service (DoS) by sending an HTTP request with a very long "ssid" parameter to the "/userRpm/popupSiteSurveyRpm.html" webpage, which crashes the router. **CVE ID : CVE-2021-26827**	N/A	O-TP--TL-W-290421/3424
tl-wr802n_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-04-2021	9.3	TP-Link TL-WR802N(US), Archer_C50v5_US v4_200 <= 2020.06 contains a buffer overflow vulnerability in the httpd process in the body message. The attack vector is: The attacker can get shell of the router by sending a message through the network, which may lead to remote code execution. **CVE ID : CVE-2021-29302**	https://static.tp-link.com/beta/2021/202103/20210319/TL-WR802Nv4_US_0.9.1_3.17_up_boot[210317-rel64474].zip, https://www.tp-link.com/us/support/download/tl-wr802n/#Firmware	O-TP--TL-W-290421/3425
tl-xdr1850_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo <	https://service.tp-link.com.cn/detail_download_8	O-TP--TL-X-290421/3426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	
tl-xdr1860_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_d	O-TP--TL-X-290421/3427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which the on-link flag is set. **CVE ID : CVE-2021-3125**	ownload_8720.html	
tl-xdr3230_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	O-TP--TL-X-290421/3428
tl-xdr3250_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html,	O-TP--TL-X-290421/3429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	
tl-xdr5430_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	https://service.tp-link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	O-TP--TL-X-290421/3430
tl-xdr6060_firmware					
Excessive Iteration	12-04-2021	4.3	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 <	https://service.tp-	O-TP--TL-X-290421/3431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. **CVE ID : CVE-2021-3125**	link.com.cn/detail_download_8724.html, https://service.tp-link.com.cn/detail_download_8722.html, https://service.tp-link.com.cn/detail_download_8725.html, https://service.tp-link.com.cn/detail_download_8720.html	
windriver					
vxworks					
Out-of-bounds Write	13-04-2021	7.5	An issue was discovered in Wind River VxWorks through 6.8. There is a possible stack overflow in dhcp server. **CVE ID : CVE-2021-29999**	https://support2.windriver.com/index.php?page=security-notices	O-WIN-VXWO-290421/3432
Out-of-bounds Write	13-04-2021	7.5	An issue was discovered in Wind River VxWorks before 6.5. There is a possible heap overflow in dhcp client. **CVE ID : CVE-2021-29998**	https://support2.windriver.com/index.php?page=security-notices	O-WIN-VXWO-290421/3433
Improper Restriction of XML External	13-04-2021	6.4	XML External Entity Resolution (XXE) in Helix ALM. The XML Import	N/A	O-WIN-VXWO-290421/3434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			functionality of the Administration console in Perforce Helix ALM 2020.3.1 Build 22 accepts XML input data that is parsed by insecurely configured software components, leading to XXE attacks. **CVE ID : CVE-2021-29997**		
zte					
zxa10_c300m_firmware					
Uncontrolled Resource Consumption	09-04-2021	5	A ZTE product has a configuration error vulnerability. Because a certain port is open by default, an attacker can consume system processing resources by flushing a large number of packets to the port, and successfully exploiting this vulnerability could reduce system processing capabilities. This affects: ZXA10 C300M all versions up to V4.3P8. **CVE ID : CVE-2021-21728**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014784	O-ZTE-ZXA1-290421/3435
zxcloud_irai_firmware					
Cross-Site Request Forgery (CSRF)	13-04-2021	5.8	A CSRF vulnerability exists in the management page of a ZTE product.The vulnerability is caused because the management page does not fully verify whether the request comes from a trusted user. The attacker could submit a malicious request to the affected device to delete the data. This affects: ZXCLOUD iRAI All versions	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014824	O-ZTE-ZXCL-290421/3436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			up to KVM-ProductV6.03.04 **CVE ID : CVE-2021-21731**		
zxhn_h108n_firmware					
Cross-Site Request Forgery (CSRF)	13-04-2021	4.3	Some ZTE products have CSRF vulnerability. Because some pages lack CSRF random value verification, attackers could perform illegal authorization operations by constructing messages.This affects: ZXHN H168N V3.5.0_EG1T5_TE, V2.5.5, ZXHN H108N V2.5.5_BTMT1 **CVE ID : CVE-2021-21729**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014904	O-ZTE-ZXHN-290421/3437
zxhn_h168n_firmware					
Cross-Site Request Forgery (CSRF)	13-04-2021	4.3	Some ZTE products have CSRF vulnerability. Because some pages lack CSRF random value verification, attackers could perform illegal authorization operations by constructing messages.This affects: ZXHN H168N V3.5.0_EG1T5_TE, V2.5.5, ZXHN H108N V2.5.5_BTMT1 **CVE ID : CVE-2021-21729**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1014904	O-ZTE-ZXHN-290421/3438