

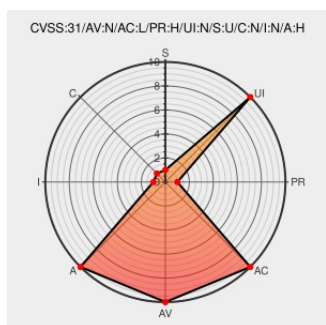


CVE-2021-28187

Published on: 04/06/2021 12:00:00 AM UTC

Last Modified on: 04/13/2021 02:57:00 PM UTC

CVE-2021-28187 - advisory for TVN-202103014

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Asmb8-ikvm](#) from [Asus](#) contain the following vulnerability:

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-2021-28187 has been assigned by [cve@cert.org.tw](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [ASUS](#) - BMC firmware for Z10PR-D16 version = 1.14.51

Affected Vendor/Software: [ASUS](#) - BMC firmware for ASMB8-iKVM version = 1.14.51

Affected Vendor/Software: [ASUS](#) - BMC firmware for Z10PE-D16 WS version = 1.14.2

CVSS3 Score: **4.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
官方支援 ASUS 台灣	www.asus.com text/html	 MISC www.asus.com/tw/support/callus/
TWCERT/CC台灣電腦網路危機處理暨協調中心-ASUS BMC's firmware: buffer overflow - 生成SSL憑證功能	www.twcert.org.tw text/html	 MISC www.twcert.org.tw/tw/cp-132-4557-1019f-1.html
ASUS Product Security Advisory ASUS Global	www.asus.com text/html	 MISC www.asus.com/content/ASUS-Product-Security-Advisory/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Asus	Asmb8-ikvm	-	All	All	All
Operating System	Asus	Asmb8-ikvm Firmware	1.14.51	All	All	All
Hardware 	Asus	Z10pe-d16 Ws	-	All	All	All
Operating System	Asus	Z10pe-d16 Ws Firmware	1.14.2	All	All	All
Hardware 	Asus	Z10pr-d16	-	All	All	All
Operating System	Asus	Z10pr-d16 Firmware	1.14.51	All	All	All

```
cpe:2.3:h:asus:asmb8-ikvm:-:*:*:*:*:*:
```

```
cpe:2.3:o:asus:asmb8-ikvm_firmware:1.14.51:****:*:*:*:
```

```
cpe:2.3:h:asus:z10pe-d16_ws:-:*****:.*.*
```

```
cpe:2.3:o:asus:z10pe-d16_ws_firmware:1.14.2:*:*:*:*:*:
```

```
cpe:2.3:h:asus:z10pr-d16:-:*:*:*:*:*:
```

```
cpe:2.3:o:asus:z10pr-d16_firmware:1.14.51:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28187 : The specific function in ASUS BMC's firmware Web management page Generate new SSL certificate do... twitter.com/i/web/status/1...	2021-04-06 05:09:52

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)