

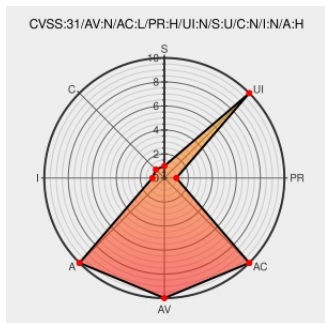


CVE-2021-28186

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

Last Modified on: 04/13/2021 02:29:00 PM UTC

CVE-2021-28186 - advisory for TVN-202103013

[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 (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-2021-28186 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.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](#)