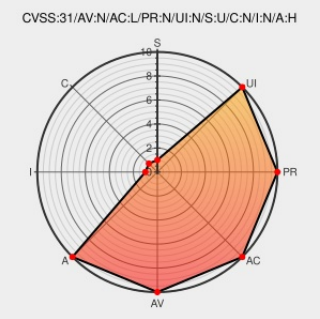
CVE-2021-31518

Published on: 05/05/2021 12:00:00 AM UTC

Last Modified on: 05/11/2021 07:05:00 PM UTC

CVE-2021-31518

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Home Network Security from Trendmicro contain the following vulnerability:

Trend Micro Home Network Security 6.5.599 and earlier is vulnerable to a file-parsing vulnerability which could allow an attacker to exploit the vulnerability and cause a denial-of-service to the device. This vulnerability is similar, but not identical to CVE-2021-31517.

CVE-2021-31518 has been assigned by security@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Trend Micro** - **Trend Micro Home Network Security** version **6.5.599 and below**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Security Bulletin: Trend Micro Home Network Security File-Parsing Denial-of-Service Vulnerabilities · Trend Micro for Home	helpcenter.trendmicro.com text/html	MISC helpcenter.trendmicro.com/en-us/article/TMKA-10312

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trendmicro	Home Network Security	All	All	All	en
Application	Trendmicro	Home Network Security	All	All	All	ja
Application	Trendmicro	Home Network Security	All	All	All	zh
Application	Trendmicro	Home Network Security	All	All	All	en
Application	Trendmicro	Home Network Security	All	All	All	ja
Application	Trendmicro	Home Network Security	All	All	All	zh

cpe:2.3:a:trendmicro:home_network_security:*:*:*:en:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:ja:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:zh:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:en:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:ja:*:*:*:*:

cpe:2.3:a:trendmicro:home_network_security:*:*:*:zh:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31518 : Trend Micro Home Network Security is vulnerable to a file-parsing vulnerability which could allow… twitter.com/i/web/status/1…	2021-05-05 15:07:52
/r/netcve	CVE-2021-31518	2021-05-05 15:41:17

← Previous ID

Next ID→

© 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 registred 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