



CVE-2020-23161

Published on: 01/22/2021 12:00:00 AM UTC

Last Modified on: 03/30/2021 01:15:00 PM UTC

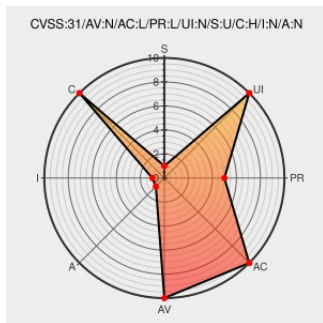
CVE-2020-23161

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Termod4** from **Pyres** contain the following vulnerability:

Local file inclusion in Pyrescom Termod4 time management devices before 10.04k allows authenticated remote attackers to traverse directories and read sensitive files via the Maintenance > Logs menu and manipulating the file-path in the URL.

CVE-2020-23161 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
GitHub - Outpost24/Pyrescom-Termod-PoC: Pyrescom Termod proof-of-concept code for CVE-2020-23160, CVE-2020-23161 and CVE-2020-23162	github.com text/html	MISC github.com/Outpost24/Pyrescom-Termod-PoC
Termod 4 - Pyrescom	Product	MISC pyres.com/en/solutions/termod-

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](#)