



CVE-2020-23162

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

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-23162

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

Certain versions of [Termod4](#) from [Pyres](#) contain the following vulnerability:

Sensitive information disclosure and weak encryption in Pyrescom Termod4 time management devices before 10.04k allows remote attackers to read a session-file and obtain plain-text user credentials.

CVE-2020-23162 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
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/termo-

Multiple vulnerabilities discovered in Pyrescom Termod4 smart device |
Outpost 24 blog

outpost24.com
text/html

MISC outpost24.com/blog/multiple-vulnerabilities-discovered-in-Pyrescom-Termod4-smart-device

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

Exploit/POC from Github

Pyrescom Termod proof-of-concept code for CVE-2020-23160, CVE-2020-23161 and CVE-2020-23162

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Pyres	Termod4	-	All	All	All
Hardware 	Pyres	Termod4	-	All	All	All
Operating System	Pyres	Termod4 Firmware	All	All	All	All
Operating System	Pyres	Termod4 Firmware	All	All	All	All
cpe:2.3:h:pyres:termod4:-:*****:						
cpe:2.3:h:pyres:termod4:-:*****:						
cpe:2.3:o:pyres:termod4_firmware:*****:						
cpe:2.3:o:pyres:termod4_firmware:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

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](#)