



CVE-2023-22620

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-22620
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-12 23:15:00 UTC
Updated	2023-04-21 15:34:00 UTC
Description	An issue was discovered in SecurePoint UTM before 12.2.5.1. The firewall's endpoint at /spcgi.cgi allows sessionid informa

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Securepoint	Unified Threat Management	All	All	All	All

References

Reference	Source
RCE Security – Remote Code Execution Techniques and more	MISC
advisories/CVE-2023-22620.txt at master · MrTuxracer/advisories · GitHub	MISC
SecurePoint UTM 12.x Session ID Leak ≈ Packet Storm	MISC
Full Disclosure: [CVE-2023-22620] SecurePoint UTM <= 12.2.5 “spcgi.cgi” sessionId Information Disclosure Allowing Device Takeover	FULL
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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