



CVE-2022-31161

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

Summary

CVE	CVE-2022-31161
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-15 21:15:00 UTC
Updated	2023-04-03 20:15:00 UTC
Description	Roxy-WI is a Web interface for managing HAProxy, Nginx and Keepalived servers. Prior to version 6.1.1.0, the system com

Risk And Classification

Problem Types: CWE-94 | CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Roxy-wi	Roxy-wi	All	All	All	All

References

Reference	Source	Link	T
Release v6.1.1.0 · hap-wi/roxy-wi · GitHub	MISC	github.com	
Roxy WI 6.1.1.0 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
Unauthenticated Remote Code Execution via ssl_cert Upload · Advisory · hap-wi/roxy-wi · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

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

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