



CVE-2021-31630

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-31630
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-03 15:15:00 UTC
Updated	2022-05-03 16:04:00 UTC
Description	Command Injection in Open PLC Webserver v3 allows remote attackers to execute arbitrary code via the "Hardware Layer

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Openplcproject	Openplc V3	-	All	All	All
Operating System	Openplcproject	Openplc V3 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
PoC - Authenticated Remote Code Execution on OpenPLC_V3 WebServer - YouTube	MISC	www.youtube.com	
OpenPLC WebServer 3 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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](#).

CVE.report and Source URL Uptime Status status.cve.report