



CVE-2019-7276

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

Summary

CVE	CVE-2019-7276
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-01 20:15:00 UTC
Updated	2023-03-28 17:15:00 UTC
Description	Optergy Proton/Enterprise devices allow Remote Root Code Execution via a Backdoor Console.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Optergy	Enterprise	All	All	All	All
Application	Optergy	Proton	All	All	All	All

References

Reference	Source	Link
Optergy Proton And Enterprise BMS 2.0.3a Command Injection ~ Packet Storm	MISC	packetstorm
Applied Risk :: Advisories	MISC	applied-risk
Optergy Proton / Enterprise Multiple Vulnerabilities Optergy Proton / Enterprise Multiple Vulnerabilities - Applied Risk	MISC	www.applied-risk.com
Optergy Proton Enterprise Building Management System Multiple Security Vulnerabilities	BID	www.securityfocus.com/bid/108881
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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