



CVE-2020-17387

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

Summary

CVE	CVE-2020-17387
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-25 21:15:00 UTC
Updated	2020-08-28 17:26:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 4.0.0.0. The vulnerability exists due to insufficient input validation. An attacker can exploit this to execute arbitrary code on the target system. (CVE-2020-17387)

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Marvell	Qconvergeconsole	All	All	All	All
Application	Marvell	Qconvergeconsole	All	All	All	All

References

Reference	Source	Link	Tags
www.marvell.com/content/dam/marvell/en/public-collateral/fibre-channel/marvell-qconvergeconsole-4.0.0.0-security-advisory.pdf	MISC	www.marvell.com	Vendor Advisory
ZDI-20-974 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)