



CVE-2020-12251

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

Summary

CVE	CVE-2020-12251
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-29 14:15:00 UTC
Updated	2020-05-18 15:47:00 UTC
Description	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an authenticated user to change

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gigamon	Gigavue	All	All	All	All
Application	Gigamon	Gigavue	All	All	All	All

References

Reference	Source	Link	Tags
Full Disclosure: Gigamon - GigaVUE 0day	MISC	seclists.org	Mailing List, Third Party
Gigamon GigaVUE 5.5.01.11 Directory Traversal / File Upload ≈ Packet Storm	MISC	packetstormsecurity.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](#).

Free CVE JSON API cve.report/api

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