CVE-2016-6255

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-6255
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-07 16:59:00 UTC
Updated	2017-11-03 01:29:00 UTC
Description	Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to write to arbitrary files in the webroot via a POST

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libupnp Project	Libupnp	All	All	All	All

References

Reference
Matthew Garrett on Twitter: "Reported this to upstream 8 months ago without response, so: libupnp's default behaviour allows anyone to write
Portable UPnP SDK / Code / [0497e6] /ChangeLog
libupnp CVE-2016-6255 Arbitrary File Write Vulnerability
libupnp: Multiple vulnerabilities (GLSA 201701-52) — Gentoo security
[R1] Debian MediaTomb (fork) Multiple Remote Vulnerabilities - Research Advisory | Tenable®
MiCasaVerde VeraLite - Remote Code Execution - Hardware remote Exploit
oss-security - Re: libupnp write files via POST
oss-security - libupnp write files via POST
Don't allow unhandled POSTs to write to the filesystem by default · mjg59/pupnp-code@be0a01b · GitHub
Debian -- Security Information -- DSA-3736-1 libupnp
CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710545 Gentoo Linux libupnp Multiple Vulnerabilities (GLSA 201701-52)