CVE-2018-19975

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

Summary

CVE	CVE-2018-19975
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-17 19:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	In YARA 3.8.1, bytecode in a specially crafted compiled rule can read data from any arbitrary address in memory, in libyara

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Virustotal	Yara	3.8.1	All	All	All
Application	Virustotal	Yara	3.8.1	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: yara-3.10.0-2.fc30 - package-announce - Fedora Mailing-Lists		lists.fedor
GitHub - bnbdr/swisscheese: PoC Exploit for YARA 3.7.1 & 3.8.1	MISC	github.cor
Compiled rules can execute malicious code regardless of PARANOID_EXEC · Issue #999 · VirusTotal/yara · GitHub	CONFIRM	github.cor
[SECURITY] Fedora 30 Update: yara-3.10.0-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
YARA Internals II: Bytecode	MISC	bnbdr.gith
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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