



CVE-2018-12035

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

Summary

CVE	CVE-2018-12035
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-15 16:29:00 UTC
Updated	2018-08-01 13:23:00 UTC
Description	In YARA 3.7.1 and prior, parsing a specially crafted compiled rule file can cause an out of bounds write vulnerability in yr_e:

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	VirusTotal	Yara	All	All	All	All

References

Reference	Source	Link	Tags
YARA Internals: Compiled Rule Format	MISC	bnbdr.github.io	Exploit, Third Party Adv
GitHub - bnbdr/swisscheese: PoC Exploit for YARA 3.7.1 & 3.8.1	MISC	github.com	Exploit, Third Party Adv
Out-of-bounds read, write in yr_execute_code · Issue #891 · VirusTotal/yara · GitHub	CONFIRM	github.com	Issue Tracking, Patch,
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