CVE-2020-10915

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10915
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-22 21:15:00 UTC
Updated	2020-05-04 19:15:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.458

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Veeam	One	9.5.4.4587	All	All	All
Application	Veeam	One	9.5.4.4587	All	All	All

References

Reference	Source	Link	Tags
KB3144: Veeam ONE Remote Code Execution Vulnerabilities	MISC	www.veeam.com	Vendor Advisory
Veeam ONE Agent .NET Deserialization ≈ Packet Storm	MISC	packetstormsecurity.com	
ZDI-20-546 | Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory, VDB Entry
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.

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