CVE-2015-2318

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

Summary

CVE	CVE-2015-2318
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-08 19:29:00 UTC
Updated	2018-01-30 19:19:00 UTC
Description	The TLS stack in Mono before 3.12.1 allows man-in-the-middle attackers to conduct message skipping attacks and conseq

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Mono-project	Mono	All	All	All	All
Application	Mono-project	Mono	All	All	All	All

References

Reference
oss-security - Re: Mono TLS vulnerabilities
USN-2547-1: Mono vulnerabilities | Ubuntu
TLS Vulnerabilities | Mono
Debian -- Security Information -- DSA-3202-1 mono
1202869 – (CVE-2015-2318, CVE-2015-2319, CVE-2015-2320) CVE-2015-2318 CVE-2015-2319 CVE-2015-2320 mono: TLS implementatior
TLS protocol: add handshake state validation · mono/mono@1509226 · GitHub
miTLS - A verified reference implementation of TLS
Mono CVE-2015-2318 Man in the Middle Spoofing Vulnerability
CVE Program record
NVD vulnerability detail

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**