



# CVE-2015-2319

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

## Summary

<b>CVE</b>	CVE-2015-2319
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-01-08 19:29:00 UTC
<b>Updated</b>	2018-01-30 19:20:00 UTC
<b>Description</b>	The TLS stack in Mono before 3.12.1 makes it easier for remote attackers to conduct cipher-downgrade attacks to EXPORT

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Mono-project</a>	<a href="#">Mono</a>	All	All	All	All
Application	<a href="#">Mono-project</a>	<a href="#">Mono</a>	All	All	All	All

## References

### Reference

- [oss-security - Re: Mono TLS vulnerabilities](#)
- [USN-2547-1: Mono vulnerabilities | Ubuntu](#)
- [TLS Vulnerabilities | Mono](#)
- [Mono CVE-2015-2319 Man in the Middle Security Bypass Vulnerability](#)
- [Debian -- Security Information -- DSA-3202-1 mono](#)
- [miTLS - A verified reference implementation of TLS](#)
- [1202869 -- \(CVE-2015-2318, CVE-2015-2319, CVE-2015-2320\) CVE-2015-2318 CVE-2015-2319 CVE-2015-2320 mono: TLS implementation](#)
- [Remove the EXPORT ciphers and related code path · mono/mono@9c38772 · GitHub](#)
- [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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)