



CVE-2018-12384

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

Summary

CVE	CVE-2018-12384
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-29 15:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-

Risk And Classification

Problem Types: CWE-335

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All

References

Reference	Source	Link
1483128 - (CVE-2018-12384) ServerHello.random is all zero when handling a v2-compatible ClientHello	CONFIRM	bugzilla.mozilla.org
Oracle Critical Patch Update - October 2019	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378164](#) Virtuozzo Linux Security Update for nss-tools (VZLSA-2018:2898)

[390279](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for nss (OVMSA-2023-0014)

[500453](#) Alpine Linux Security Update for nss

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)