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-z

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