CVE-2020-12402

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12402
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-09 15:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which er

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link	Tags
Mozilla Firefox: Multiple vulnerabilities (GLSA 202007-10) — Gentoo security	GENTOO	security.gentoo.org	Third F
[security-announce] openSUSE-SU-2020:0955-1: moderate: Security update f	SUSE	lists.opensuse.org	Third F
[security-announce] openSUSE-SU-2020:0983-1: important: Security update	SUSE	lists.opensuse.org	Third F
USN-4417-1: NSS vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third F
Access Denied	MISC	bugzilla.mozilla.org	Issue T

USN-4417-2: NSS vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third F
[SECURITY] Fedora 31 Update: nss-3.54.0-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third F
[SECURITY] Fedora 32 Update: nspr-4.26.0-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 31 Update: nss-3.54.0-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Security Vulnerabilities fixed in Firefox 78 — Mozilla	MISC	www.mozilla.org	Vendo
Debian -- Security Information -- DSA-4726-1 nss	DEBIAN	www.debian.org	Third F
[SECURITY] Fedora 32 Update: nspr-4.26.0-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third F
[security-announce] openSUSE-SU-2020:1017-1: important: Security update	SUSE	lists.opensuse.org	Third F
[SECURITY] [DLA 2388-1] nss security update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2020:0953-1: moderate: Security update f	SUSE	lists.opensuse.org	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 296071 Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)
- 352469 Amazon Linux Security Advisory for nspr, nss-softokn, nss-util: ALAS-2021-1522
- 377524 Alibaba Cloud Linux Security Update for nss and nspr (ALINUX2-SA-2020:0173)
- 500457 Alpine Linux Security Update for nss
- 500951 Alpine Linux Security Update for firefox
- 503836 Alpine Linux Security Update for firefox
- 670373 EulerOS Security Update for nss (EulerOS-SA-2021-1952)
- 670394 EulerOS Security Update for nss (EulerOS-SA-2021-1931)
- 940400 AlmaLinux Security Update for nss and nspr (ALSA-2020:3280)
- 960710 Rocky Linux Security Update for nss and nspr (RLSA-2020:3280)