CVE-2020-12403

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12403
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-27 19:15:00 UTC
Updated	2023-03-24 16:15:00 UTC
Description	A flaw was found in the way CHACHA20-POLY1305 was implemented in NSS in versions before 3.55. When using multi-pa

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Nss	All	All	All	All

References

Reference	S
NSS 3.55 release notes - Mozilla | MDN	M
[SECURITY] [DLA 3327-1] nss security update	M
1868931 – (CVE-2020-12403) CVE-2020-12403 nss: CHACHA20-POLY1305 decryption with undersized tag leads to out-of-bounds read	M
CVE-2020-12403 Libnss Vulnerability in NetApp Products | NetApp Product Security	C
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181594 Debian Security Update for nss (DLA 3327-1)

239173 Red Hat Update for nss and nss-softokn (RHSA-2021:0876)

239184 Red Hat Update for nss-softokn (RHSA-2021:1026)

352469 Amazon Linux Security Advisory for nspr, nss-softokn, nss-util: ALAS-2021-1522

377391 Alibaba Cloud Linux Security Update for nss (ALINUX3-SA-2021:0015)

377524 Alibaba Cloud Linux Security Update for nss and nspr (ALINUX2-SA-2020:0173)

500458 Alpine Linux Security Update for nss

900037 CBL-Mariner Linux Security Update for nss 3.44

901861 Common Base Linux Mariner (CBL-Mariner) Security Update for nss (6746-1)

903133 Common Base Linux Mariner (CBL-Mariner) Security Update for nss (4326)

904928 Common Base Linux Mariner (CBL-Mariner) Security Update for openjdk8 (12402)

904973 Common Base Linux Mariner (CBL-Mariner) Security Update for mozjs60 (12364)

940393 AlmaLinux Security Update for nss (ALSA-2021:0538)

960725 Rocky Linux Security Update for nss (RLSA-2021:0538)