# CVE-2020-25648

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-25648 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-10-20 22:15:00 UTC |
| **Updated** | 2023-11-07 03:20:00 UTC |
| **Description** | A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This flaw allows a remote attac |

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Mozilla | Network Security Services | All | All | All | All |
| Application | Mozilla | Network Security Services | All | All | All | All |
| Application | Oracle | Communications Offline Mediation Controller | 12.0.0.3.0 | All | All | All |
| Application | Oracle | Communications Pricing Design Center | 12.0.0.3.0 | All | All | All |
| Application | Oracle | Jd Edwards Enterpriseone Tools | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| 1887319 – (CVE-2020-25648) CVE-2020-25648 nss: TLS 1.3 CCS flood remote DoS Attack | MISC | bugzilla.redhat.co |
| [SECURITY] Fedora 32 Update: nss-3.58.0-3.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| Oracle Critical Patch Update Advisory - April 2022 | MISC | www.oracle.com |
| Pony Mail! | MLIST | lists.apache.org |
| Oracle Critical Patch Update Advisory - July 2021 | N/A | www.oracle.com |
| NSS 3.58 release notes - Mozilla \| MDN | MISC | developer.mozilla. |
| Oracle Critical Patch Update Advisory - October 2021 | MISC | www.oracle.com |
| [SECURITY] Fedora 31 Update: nss-3.58.0-3.fc31 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| [SECURITY] Fedora 31 Update: nss-3.58.0-3.fc31 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| [SECURITY] Fedora 33 Update: nss-3.58.0-3.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| [SECURITY] [DLA 3634-1] nss security update | MLIST | lists.debian.org |
| [mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar | | lists.apache.org |
| [SECURITY] Fedora 32 Update: nss-3.58.0-3.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| [SECURITY] Fedora 33 Update: nss-3.58.0-3.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| 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

- 159168 Oracle Enterprise Linux Security Update for nss (ELSA-2021-1384)
- 159395 Oracle Enterprise Linux Security Update for nss and nspr (ELSA-2021-3572)
- 198779 Ubuntu Security Notification for NSS Vulnerability (USN-5410-1)
- 239252 Red Hat Update for nss (RHSA-2021:1384)
- 239650 Red Hat Update for nss and nspr (RHSA-2021:3572)
- 352390 Amazon Linux Security Advisory for nss: ALAS2-2021-1664
- 352473 Amazon Linux Security Advisory for nss: ALAS-2021-1518
- 377407 Alibaba Cloud Linux Security Update for nss and nspr (ALINUX3-SA-2021:0071)
- 377470 Alibaba Cloud Linux Security Update for nss (ALINUX2-SA-2021:0025)
- 500459 Alpine Linux Security Update for nss
- 6000253 Debian Security Update for nss (DLA 3634-1)
- 710087 Gentoo Linux Mozilla Network Security Service (NSS) Denial of service vulnerability (GLSA 202012-21)

730155 McAfee Web Gateway Multiple Vulnerabilities(WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934,WP-3935, WP-3936, WP-3999)

940251 AlmaLinux Security Update for nss and nspr (ALSA-2021:3572)

960023 Rocky Linux Security Update for nss and nspr (RLSA-2021:3572)