CVE-2020-6829

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-6829
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-28 12:15:00 UTC
Updated	2023-02-20 17:15:00 UTC
Description	When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial info

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Security Vulnerabilities fixed in Firefox 80 — Mozilla	MISC	www.mozilla.org	Vendor Advisory
Access Denied	MISC	bugzilla.mozilla.org	Permissions Required
Security Vulnerabilities fixed in Firefox for Android 80 — Mozilla	MISC	www.mozilla.org	Vendor Advisory
[SECURITY] [DLA 3327-1] nss security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

500953 Alpine Linux Security Update for firefox

503838 Alpine Linux Security Update for firefox

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

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