CVE-2016-1938

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-1938
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-31 18:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The s_mp_div function in lib/freebl/mpi/mpi.c in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Fir

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Nss	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference
Errors in mp_div and mp_exptmod cryptographic functions in NSS — Mozilla
[security-announce] openSUSE-SU-2016:0306-1: important: Security update
1190248 - (CVE-2016-1938) mp_div and mp_exptmod sometimes produce wrong calculation results
Oracle Critical Patch Update - July 2016
bignum-fuzz/CVE-2016-1938-nss-mp_exptmod.c at master · hannob/bignum-fuzz · GitHub
USN-2880-2: Firefox regression | Ubuntu

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities
[security-announce] SUSE-SU-2016:0338-1: important: Security update for
nss: diff lib/freebl/mpi/mpi.c
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security
[security-announce] openSUSE-SU-2016:0309-1: important: Security update
NSS 3.21 release notes - Mozilla | MDN
USN-2973-1: Thunderbird vulnerabilities | Ubuntu
USN-2903-2: NSS regression | Ubuntu
Debian -- Security Information -- DSA-3688-1 nss
USN-2903-1: NSS vulnerability | Ubuntu
Mozilla Network Security Service (NSS): Multiple vulnerabilities (GLSA 201701-46) — Gentoo security
Mozilla Network Security Services CVE-2016-1938 Weak Encryption Multiple Security Weaknesses
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof the Address Bar, Bypass Security Restrictions, and Deny Ser
1194947 - miscalculation in mp_exptmod()
USN-2880-1: Firefox vulnerabilities | Ubuntu
bignum-fuzz/CVE-2016-1938-nss-mp_div.c at master · hannob/bignum-fuzz · GitHub
Mozilla NSS: Wrong calculation results in mp_div() and mp_exptmod() | The Fuzzing Project
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710518 Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201701-46)