CVE-2017-5462

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-5462
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal state V does not c

Risk And Classification

Problem Types: CWE-682

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	52.0	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	52.0	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References

Reference
Security vulnerabilities fixed in Thunderbird 52.1 — Mozilla
Mozilla Firefox Multiple Bugs Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, Deny Ser

1345089 - (CVE-2017-5462) DRBG addition is broken
Security vulnerabilities fixed in Firefox 53 — Mozilla
Mozilla Network Security Service (NSS): Multiple vulnerabilities (GLSA 201705-04) — Gentoo security
Mozilla Firefox Multiple Security Vulnerabilities
Security vulnerabilities fixed in Firefox ESR 45.9 — Mozilla
Debian -- Security Information -- DSA-3872-1 nss
Security vulnerabilities fixed in Firefox ESR 52.1 — Mozilla
Debian -- Security Information -- DSA-3831-1 firefox-esr
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

690289 Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

710287 Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201802-03)

710397 Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201705-04)