CVE-2017-5375

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5375
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2018-08-02 19:35:00 UTC
Description	JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. Th

Risk And Classification

Problem Types: CWE-119

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	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference
Red Hat Customer Portal
Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution - Windows remote Exploit
Mozilla Firefox Multiple Bugs Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, and Exec
Mozilla Firefox: Multiple vulnerabilities (GLSA 201702-22) — Gentoo Security
Firefox 44.0.2 - ASM.JS JIT-Spray Remote Code Execution - Windows remote Exploit
Mozilla Firefox CVE-2017-5375 ASLR and DEP Security Bypass Vulnerability
Security vulnerabilities fixed in Thunderbird 45.7 — Mozilla
Debian -- Security Information -- DSA-3832-1 icedove
Debian -- Security Information -- DSA-3771-1 firefox-esr
Security vulnerabilities fixed in Firefox 51 — Mozilla
Firefox 46.0.1 - ASM.JS JIT-Spray Remote Code Execution - Windows remote Exploit
Red Hat Customer Portal
Mozilla Thunderbird: Multiple vulnerabilities (GLSA 201702-13) — Gentoo Security
Access Denied
Security vulnerabilities fixed in Firefox ESR 45.7 — Mozilla
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378238 Virtuozzo Linux Security Update for firefox (VZLSA-2017:0190)

378298 Virtuozzo Linux Security Update for thunderbird (VZLSA-2017:0238)

710433 Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 201702-13)

710488 Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201702-22)