CVE-2013-1620

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-1620
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-08 19:55:00 UTC
Updated	2022-12-21 17:30:00 UTC
Description	The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side-channel attacks

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
Application	Mozilla	Network Security Services	All	All	All	All
Application	Oracle	Enterprise Manager Ops Center	11.1	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.1	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2	All	All	All
Application	Oracle	Glassfish Communications Server	2.0	All	All	All
Application	Oracle	Glassfish Server	2.1.1	All	All	All
Application	Oracle	Iplanet Web Proxy Server	4.0	All	All	All
Application	Oracle	Iplanet Web Server	6.1	All	All	All
Application	Oracle	Iplanet Web Server	7.0	All	All	All
Application	Oracle	Opensso	3.0-03	All	All	All
Application	Oracle	Traffic Director	11.1.1.6.0	All	All	All
Application	Oracle	Traffic Director	11.1.1.7.0	All	All	All

Application	Oracle	Vm Server	3.2	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 Eus	5.9	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 Aus	5.9	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

References

Reference	Source	Link
USN-1763-1: NSS vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
VMSA-2014-0012 | United States	CONFIRM	www.vmware.co
Oracle Critical Patch Update - January 2014	CONFIRM	www.oracle.com
Mozilla Network Security Services CVE-2013-1620 Information Disclosure Vulnerability	BID	www.securityfocu
Oracle Critical Patch Update - April 2014	CONFIRM	www.oracle.com
Oracle Critical Patch Update - January 2015	CONFIRM	www.oracle.com
Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities	FULLDISC	seclists.org
Oracle VM Server for x86 Bulletin - July 2016	CONFIRM	www.oracle.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	CONFIRM	kb.juniper.net
Gentoo Linux Documentation -- Mozilla Network Security Service: Multiple vulnerabilities	GENTOO	security.gentoo.c
Red Hat Customer Portal	REDHAT	rhn.redhat.com
[security-announce] openSUSE-SU-2013:0630-1: important: Mozilla Firefox	SUSE	lists.opensuse.or
RETIRED: Oracle January 2014 Critical Patch Update Multiple Vulnerabilities	BID	www.securityfocu
Oracle Critical Patch Update - July 2014	CONFIRM	www.oracle.com
SecurityFocus	BUGTRAQ	www.securityfocu
[security-announce] openSUSE-SU-2013:0631-1: important: Mozilla Firefox	SUSE	lists.opensuse.or
oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations	MLIST	openwall.com
www.isg.rhul.ac.uk/tls/TLStiming.pdf	MISC	www.isg.rhul.ac.u
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report