CVE-2013-2566

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-2566
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-03-15 21:55:00 UTC
Updated	2020-11-23 19:48:00 UTC
Description	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for r

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Hardware	Fujitsu	M10-1	-	All	All	All
Hardware	Fujitsu	M10-1	-	All	All	All
Operating System	Fujitsu	M10-1 Firmware	All	All	All	All
Operating System	Fujitsu	M10-1 Firmware	All	All	All	All
Hardware	Fujitsu	M10-4	-	All	All	All
Hardware	Fujitsu	M10-4	-	All	All	All
Hardware	Fujitsu	M10-4s	-	All	All	All
Hardware	Fujitsu	M10-4s	-	All	All	All
Operating System	Fujitsu	M10-4s Firmware	All	All	All	All

Operating System	Fujitsu	M10-4s Firmware	All	All	All	All
Operating System	Fujitsu	M10-4 Firmware	All	All	All	All
Operating System	Fujitsu	M10-4 Firmware	All	All	All	All
Hardware	Fujitsu	Sparc Enterprise M3000	-	All	All	All
Hardware	Fujitsu	Sparc Enterprise M3000	-	All	All	All
Operating System	Fujitsu	Sparc Enterprise M3000 Firmware	All	All	All	All
Operating System	Fujitsu	Sparc Enterprise M3000 Firmware	All	All	All	All
Hardware	Fujitsu	Sparc Enterprise M4000	-	All	All	All
Hardware	Fujitsu	Sparc Enterprise M4000	-	All	All	All
Operating System	Fujitsu	Sparc Enterprise M4000 Firmware	All	All	All	All
Operating System	Fujitsu	Sparc Enterprise M4000 Firmware	All	All	All	All
Hardware	Fujitsu	Sparc Enterprise M5000	-	All	All	All
Hardware	Fujitsu	Sparc Enterprise M5000	-	All	All	All
Operating System	Fujitsu	Sparc Enterprise M5000 Firmware	All	All	All	All
Operating System	Fujitsu	Sparc Enterprise M5000 Firmware	All	All	All	All
Hardware	Fujitsu	Sparc Enterprise M8000	-	All	All	All
Hardware	Fujitsu	Sparc Enterprise M8000	-	All	All	All
Operating System	Fujitsu	Sparc Enterprise M8000 Firmware	All	All	All	All
Operating System	Fujitsu	Sparc Enterprise M8000 Firmware	All	All	All	All
Hardware	Fujitsu	Sparc Enterprise M9000	-	All	All	All
Hardware	Fujitsu	Sparc Enterprise M9000	-	All	All	All
Operating System	Fujitsu	Sparc Enterprise M9000 Firmware	All	All	All	All
Operating System	Fujitsu	Sparc Enterprise M9000 Firmware	All	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	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Application	Oracle	Communications Application Session Controller	All	All	All	All
Application	Oracle	Http Server	11.1.1.7.0	All	All	All

Application	Oracle	Http Server	11.1.1.9.0	All	All	All
Application	Oracle	Http Server	12.1.3.0.0	All	All	All
Application	Oracle	Http Server	12.2.1.1.0	All	All	All
Application	Oracle	Http Server	12.2.1.2.0	All	All	All
Application	Oracle	Http Server	11.1.1.7.0	All	All	All
Application	Oracle	Http Server	11.1.1.9.0	All	All	All
Application	Oracle	Http Server	12.1.3.0.0	All	All	All
Application	Oracle	Http Server	12.2.1.1.0	All	All	All
Application	Oracle	Http Server	12.2.1.2.0	All	All	All
Operating System	Oracle	Integrated Lights Out Manager Firmware	All	All	All	All
Operating System	Oracle	Integrated Lights Out Manager Firmware	All	All	All	All

References

Reference	Source	Link
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	www.oracl
Welcome - Opera Security Corner	CONFIRM	www.opera
SSL/TLS RC4 CVE-2013-2566 Information Disclosure Weakness	BID	www.secu
Oracle Critical Patch Update - July 2016	CONFIRM	www.oracl
Document Display | HPE Support Center	CONFIRM	h20566.ww
MFSA 2013-103: Miscellaneous Network Security Services (NSS) vulnerabilities	CONFIRM	www.mozil
cr.yp.to/talks/2013.03.12/slides.pdf	MISC	cr.yp.to
USN-2032-1: Thunderbird vulnerabilities | Ubuntu	UBUNTU	www.ubun
Gentoo Security	GENTOO	security.ge
Oracle Critical Patch Update - January 2018	CONFIRM	www.oracl
Oracle Critical Patch Update - October 2016	CONFIRM	www.oracl
The Opera Security group - On the Precariousness of RC4	CONFIRM	my.opera.c
'[security bulletin] HPSBGN03324 rev.1 - HP Business Service Automation Essentials Core, Remote Discl' - MARC	HP	marc.info
Document Display | HPE Support Center	CONFIRM	h20566.ww
Gentoo Linux Documentation -- Mozilla Network Security Service: Multiple vulnerabilities	GENTOO	security.ge
On the Security of RC4 in TLS	MISC	www.isg.rh
A Few Thoughts on Cryptographic Engineering: Attack of the week: RC4 is kind of broken in TLS	MISC	blog.crypto
USN-2031-1: Firefox vulnerabilities | Ubuntu	UBUNTU	www.ubun
Opera for Mobile Devices	CONFIRM	www.opera
Oracle Critical Patch Update - October 2017	CONFIRM	www.oracl
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	kb.juniper.
CVE Program record	CVE.ORG	www.cve.o

NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591186 Mitsubishi Electric Air Conditioning Systems Multiple Vulnerabilities (ICSA-22-160-01)