CVE-2011-3389

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-3389
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-06 19:55:00 UTC
Updated	2022-11-29 15:56:00 UTC
Description	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, G

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	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	-	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Haxx	Curl	All	All	All	All
Application	Microsoft	Ie	All	All	All	All
Application	Microsoft	Ie	All	All	All	All
Application	Microsoft	Internet Explorer	All	All	All	All
Application	Microsoft	Internet Explorer	-	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	-	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Opera	Opera Browser	All	All	All	All
Application	Opera	Opera Browser	-	All	All	All
Application	Opera	Opera Browser	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 Eus	6.2	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	6.2	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
Hardware	Siemens	Simatic Rf615r	-	All	All	All
Operating System	Siemens	Simatic Rf615r Firmware	All	All	All	All
Hardware	Siemens	Simatic Rf68xr	-	All	All	All
Operating System	Siemens	Simatic Rf68xr Firmware	All	All	All	All

References

Reference
IBM WebSphere DataPower Lets Remote Users Decrypt SSL/TLS Traffic - SecurityTracker
About the security content of OS X Mavericks v10.9.2 and Security Update 2014-001 - Apple Support
APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4
APPLE-SA-2012-02-01-1 OS X Lion v10.7.3 and Security Update 2012-001
cURL - Security Advisory (SSL CBC IV vulnerability)
About Secunia Research | Flexera
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability
Repository / Oval Repository
Red Hat Customer Portal
APPLE-SA-2012-09-19-2 OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004
'[security bulletin] HPSBMU02797 SSRT100867 rev.1 - HP Network Node Manager i (NNMi) v9.1x Running JD' - MARC
AST-2016-001
About Secunia Research | Flexera
Multiple vulnerabilities in fetchmail (Third Party Vulnerability Resolution Blog)

About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004

The Opera Security group - The "BEAST" SSL/TLS issue

Gentoo Linux Documentation -- cURL: Multiple vulnerabilities

Cryptology ePrint Archive: Report 2006/136

developerWorks : Java™; technology : IBM developer kits : Additional documentation

APPLE-SA-2013-10-22-3 OS X Mavericks v10.9

[security-announce] SUSE-SU-2012:0602-1: important: Security update for

theagora.io

Security Advisory SA48256 - Gentoo update for curl - Secunia

APPLE-SA-2011-10-12-1 iOS 5 Software Update

Opera 11.51 for Mac changelog

Oracle Critical Patch Update - July 2015

Debian -- Security Information -- DSA-2398-2 curl

Philips Intellispace Portal ISP Vulnerabilities | ICS-CERT

About Secunia Research | Flexera

Opera 11.51 for UNIX changelog

737506 – (BEAST, CVE-2011-3389) CVE-2011-3389 HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST)

SecurityTracker: Microsoft Windows SSL/TLS Protocol Flaw Lets Remote Users Decryption Sessions

About Secunia Research | Flexera

[security-announce] openSUSE-SU-2020:0086-1: important: Security update

About Secunia Research | Flexera

Attack against TLS-protected communications at Mozilla Security Blog

Access Denied

'[security bulletin] HPSBMU02742 SSRT100740 rev.1 - HP System Management Homepage (SMH) for Linux and' - MARC

cert-portal.siemens.com/productcert/pdf/ssa-556833.pdf

Opera 11.60 for Mac changelog

US-CERT Alert TA12-010A - Microsoft Updates for Multiple Vulnerabilities

'[security bulletin] HPSBUX02730 SSRT100710 rev.1 - HP-UX Running Java, Remote Unauthorized Access, D' - MARC

access.redhat.com

Oracle Critical Patch Update - January 2015

Microsoft Security Advisory 2588513 | Microsoft Docs

[security-announce] SUSE-SU-2012:0122-1: important: Security update for

Opera 11.60 for Windows changelog

About the security content of OS X Lion v10.7.4 and Security Update 2012-002

ISC Diary | SSL/TLS (part 3)

Opera 11.60 for UNIX changelog

[security-announce] SUSE-SU-2012:0114-1: important: Security update for

ekoparty Security Conference

Security Advisory SA55351 - Oracle Forms and Reports Two Weaknesses - Secunia

APPLE-SA-2012-05-09-1 OS X Lion v10.7.4 and Security Update 2012-002

'[security bulletin] HPSBUX02777 SSRT100854 rev.1 - HP-UX Running Java JRE and JDK, Remote Denial' - MARC

SecurityTracker: Opera Lets Remote Users Spoof Extended Validation Address Bar Security Information and Decrypt SSL/TLS Traffic

openSUSE-SU-2012:0030

About the security content of iOS 5 Software Update

VU#864643 - SSL 3.0 and TLS 1.0 allow chosen plaintext attack in CBC modes

Opera Web Browser Information Disclosure Vulnerability

About the security content of OS X Lion v10.7.3 and Security Update 2012-001

Red Hat Customer Portal

Microsoft releases Security Advisory 2588513 - MSRC - Site Home - TechNet Blogs

thái: BEAST

openSUSE-SU-2012:0063

Microsoft Security Bulletin MS12-006 - Important | Microsoft Docs

Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities

'[security bulletin] HPSBMU02799 SSRT100867 rev.1 - HP Network Node Manager i (NNMi) v9.0x Running JD' - MARC

A weakness in the SSL v3.0 and TLS 1.0 specifications can allow eavesdropping attacks against some applications - Opera Knowledge Base

Oracle Java Critical Patch Update - October 2011

Opera 11.51 for Windows changelog

HPSBMU02900

access.redhat.com

Is SSL broken? – More about Security Advisory 2588513 - Security Research & Defense - Site Home - TechNet Blogs

'[security bulletin] HPSBUX02760 SSRT100805 rev.1 - HP-UX Running Java, Remote Unauthorized Access, D' - MARC

USN-1263-1: IcedTea-Web, OpenJDK 6 vulnerabilities | Ubuntu

About the security content of Apple TV Software Update 4.4

Security impact of the Rizzo/Duong CBC "BEAST" attack - Educated Guesswork

Please wait...

Oracle Fusion Middleware Flaws Let Remote Users Deny Service and Partially Access and Modify Data - SecurityTracker

www.mandriva.com

74829

APPLE-SA-2012-07-25-2 Xcode 4.4

Cryptology ePrint Archive: Report 2004/111

Security Advisory SA55350 - Oracle Fusion Middleware Two Information Disclosure Weaknesses - Secunia

ImperialViolet - Chrome and the BEAST
About Secunia Research | Flexera
About Secunia Research | Flexera
Chrome Releases: Chrome Stable Release
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

390279 Oracle Managed Virtualization (VM) Server for x86 Security Update for nss (OVMSA-2023-0014)