CVE-2009-3555

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2009-3555
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-11-09 17:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
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	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
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	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	F5	Nginx	All	All	All	All
Operating System	Fedoraproject	Fedora	11	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Operating System	Fedoraproject	Fedora	11	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Application	Mozilla	Nss	All	All	All	All
Application	Openssl	Openssl	1.0	All	openvms	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0	All	openvms	All

References

Reference
OpenOffice.org Data Manipulation and Code Execution Vulnerabilities - Advisories - Community
Support | Red Hat
ASA-2010-119 (RHSA-2010-0165)
CTX123359 - Transport Layer Security Renegotiation Vulnerability - Citrix Knowledge Center
ProFTPD TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com
oss-security - Re: CVE-2009-3555 for TLS renegotiation MITM attacks
'[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC
[SECURITY] Fedora 11 Update: tomcat-native-1.1.18-1.fc11
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Microsoft Security Bulletin MS10-049 - Critical | Microsoft Docs
Mozilla Firefox Multiple Vulnerabilities - Advisories - Community
Red Hat Customer Portal

Red Hat Customer Portal

HP-UX update for OpenSSL - Secunia Advisories - Vulnerability Information - Secunia.com

support.zeus.com/zws/media/docs/4.3/RELEASE_NOTES

kb.bluecoat.com/index

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Cisco Unified SIP Phones Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Mi

[TLS] MITM attack on delayed TLS-client auth through renegotiation

IBM WebSphere MQ Internet Pass-Thru TLS Renegotiation Vulnerability - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian -- Security Information -- DSA-1934-1 apache2

SecurityTracker.com Archives - Cisco Video Surveillance Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Mid

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

US-CERT Technical Cyber Security Alert TA10-287A -- Oracle Updates for Multiple Vulnerabilities

About Secunia Research | Flexera

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Slackware update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com

Support | Red Hat

Red Hat update for java-1.5.0-ibm - Advisories - Community

1021752

SecurityFocus

Links » Another Protocol Bites The Dust

[SECURITY] Fedora 11 Update: openssl-0.9.8n-1.fc11

SecurityTracker.com Archives - OpenBSD Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-in-the-Middle Attacks

sysoev.ru/nginx/patch.cve-2009-3555.txt

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat Customer Portal

Debian -- Security Information -- DSA-3253-1 pound

www.openssl.org/news/secadv_20091111.txt

[SECURITY] Fedora 12 Update: httpd-2.2.14-1.fc12

SecurityTracker.com Archives - Cisco Content Switching Module Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-

Red Hat update for JBoss Enterprise Web Server - Advisories - Community

oss-security - Re: CVEs for nginx

HP System Management Homepage Multiple Vulnerabilities - Advisories - Community

Advisories:rPSA-2009-0155 - rPath Wiki

About the security content of Java for Mac OS X 10.6 Update 2

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

About Secunia Research | Flexera

#273350: Security Vulnerability in the Transport Layer Security (TLS) and Secure Sockets Layer 3.0 (SSLv3) Protocols Involving Handshake F

HPSBGN02562 SSRT090249 rev.1 - HP ProCurve Threat Management Services (TMS) zl Module J9155A and J9156A running TLS/SSL, Re

Opera: Opera 10.60 (with Opera Widgets for Desktop) for UNIX changelog

[SECURITY] Fedora 10 Update: nginx-0.7.64-1.fc10

Cosminexusにおける複数の脆弱性：ソフトウェア製品セキュリティ情報：ソフトウェア：日立

Ubuntu update for nss - Advisories - Community

SecurityTracker.com Archives - Citrix Products Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle Attack

F5 Products TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

Repository / Oval Repository

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Sun Java System Web Proxy Server Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-in-

'[security bulletin] HPSBUX02498 SSRT090264 rev.1 - HP-UX Running Apache, Remote Unauthorized Data In' - MARC

US-CERT Technical Cyber Security Alert TA10-222A -- Microsoft Updates for Multiple Vulnerabilities

[SECURITY] Fedora 13 Update: java-1.6.0-openjdk-1.6.0.0-43.1.8.2.fc13

SecurityTracker.com Archives - Cisco Wireless Location Appliance Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-i

SSRT100179

SecurityTracker.com Archives - Cisco Application Networking Manager Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct M

Links » SSL MitM Attack, Part 2

Cisco Multiple Products TLS Session Renegotiation Plaintext Injection - Advisories - Community

rhn.redhat.com | Red Hat Support

[security-announce] SUSE-SU-2011:0847-1: important: Security update for

Repository / Oval Repository

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Frequency X Blog

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Advisories | Mandriva

NEOHAPSIS - Peace of Mind Through Integrity and Insight

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

HPSBMA02568

526689 – (CVE-2009-3555) SSL3 & TLS Renegotiation Vulnerability

Red Hat Customer Portal

Indiscreet tweet trips awareness of Web SSL vulnerability | Security News - Betanews

SecurityTracker.com Archives - IBM WebSphere MQ Internet pass-thru Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-

Apache Mail Archives

SecurityFocus

Red Hat Customer Portal

[SECURITY] Fedora 12 Update: nginx-0.7.64-1.fc12

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Support

The Secure Goose: TLS renegotiation vulnerability (CVE-2009-3555)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

ASA-2009-548

SecurityTracker.com Archives - CiscoWorks Wireless LAN Solution Engine (WLSE) Protocol Flaw in SSL Renegotiation May Let Remote Use

SecurityTracker.com Archives - Cisco Telepresence Recording Server Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct M

Sun Solaris OpenSSL TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.cc

VMSA-2011-0003

USN-927-5: nspr update | Ubuntu

Hitachi Products Multiple Vulnerabilities - Advisories - Community

ZWS 4.3r5 released (News)

Red Hat update for java-1.5.0-ibm - Advisories - Community

oss-security - Re: [TLS] CVE-2009-3555 for TLS renegotiation MITM attacks

Fedora update for httpd - Advisories - Community

[SECURITY] Fedora 12 Update: nss-util-3.12.5-1.fc12.1

62210

Red Hat Customer Portal

SUSE Update for Multiple Packages - Advisories - Community

Red Hat Customer Portal

Debian update for apache2 - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[security-announce] SUSE Security Announcement: IBM Java 1.4.2 (SUSE-SA:

[security-announce] SUSE Security Announcement: openssl (SUSE-SA:2009:05

Apache Mail Archives

rhn.redhat.com | Red Hat Support

About Secunia Research | Flexera

Security Advisories | Mandriva Linux

SecurityTracker.com Archives - Cisco Wireless LAN Controller Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-th

Pony Mail!

545755 - Update Mozilla stable branches to NSS 3.12.6 and minimal support for RFC 5746

545755 – Update Mozilla stable branches to NSS 3.12.6 and minimal support for RFC 5746

[security-announce] openSUSE-SU-2011:0845-1: important: compat-openssl09

About Security Update 2010-001

Red Hat Customer Portal

Document Display | HPE Support Center

[SECURITY] Fedora 12 Update: tomcat-native-1.1.18-1.fc12

APPLE-SA-2010-01-19-1 Security Update 2010-001

Red Hat Customer Portal

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Extended Subset » Blog Archive » Authentication Gap in TLS Renegotiation

Repository / Oval Repository

IBM IC68054: SECURITY: TRANSPORT LAYER SECURITY (TLS) HANDSHAKE RENEGOTIATION WEAK SECURITY CVE-2009-3555 - U

IBM IC67848: SECURITY: TRANSPORT LAYER SECURITY (TLS) HANDSHAKE RENEGOTIATIONWEAK SECURITY CVE-2009-3555 - Un

[SECURITY] Fedora 14 Update: java-1.6.0-openjdk-1.6.0.0-44.1.9.1.fc14

60521

BlackBerry Enterprise Server Multiple Vulnerabilities - Secunia.com

Red Hat Customer Portal

Nothing found for Support Alerts Aid 020810 Txt

SecurityTracker.com Archives - Cisco Unified Contact Center Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the

SecurityTracker.com Archives - Cisco Application Control Engine Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in

Sun Java System Products TLS Session Renegotiation Plaintext Injection - Advisories - Community

SecurityTracker.com Archives - Cisco Application Velocity System Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-i

About Secunia Research | Flexera

'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC

HP ProCurve Threat Management Services zl Module TLS/SSL Vulnerability - Advisories - Community

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:024

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities

SecurityTracker.com Archives - Cisco IOS Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle Attacks

IBM Search results - United States

OpenBSD 4.5 errata

Support | Red Hat

GnuTLS TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

Gentoo Linux Documentation -- nginx: Multiple vulnerabilities

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:012

rhn.redhat.com | Red Hat Support

[SECURITY] Fedora 12 Update: java-1.6.0-openjdk-1.6.0.0-41.1.8.2.fc12

Oracle Java SE and Java for Business Critical Patch Update Advisory - October 2010

SUSE update for openssl - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat Customer Portal

[SECURITY] Fedora 11 Update: httpd-2.2.15-1.fc11.1

'[security bulletin] HPSBHF02706 SSRT100613 rev.1 - HP Integrated Lights-Out iLO2 and iLO3 running SS' - MARC

rhn.redhat.com | Red Hat Support

rhn.redhat.com | Red Hat Support

MFSA 2010-22: Update NSS to support TLS renegotiation indication

Security

cpuapr2011

SecurityTracker.com Archives - Cisco Secure Access Control Server Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Ma

HP System Management Homepage Multiple Vulnerabilities - Advisories - Community

IBM DB2 Data Manipulation and Buffer Overflow Vulnerabilities - Advisories - Community

Ubuntu update for openjdk-6 - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM - Security Vulnerabilities and HIPER APARs fixed in DB2 for Linux, UNIX, and Windows Version 9.7 Fix Pack 2

Pony Mail!

Oracle Open Office Multiple Vulnerabilities - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Support

Red Hat Customer Portal

Red Hat Customer Portal

Thoughts on the TLS bug « Chris Paget's Blog

USN-1010-1: OpenJDK vulnerabilities | Ubuntu

Links » SSL MitM, Day 4

SecurityTracker.com Archives - Cisco ASA Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle Attacks

SecurityTracker.com Archives - CiscoWorks Common Services Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-th

[TLS] TLS renegotiation issue

About the security content of Java for Mac OS X 10.5 Update 7

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011

Apache Mail Archives

SecurityTracker.com Archives - Cisco Security Agent Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Community

Bug 533125 – CVE-2009-3555 TLS: MITM attacks via session renegotiation

[SECURITY] Fedora 13 Update: httpd-2.2.15-1.fc13

Red Hat Customer Portal

Apple Mac OS X update for Java - Advisories - Community

CVE-2009-3555

Mozilla SeaMonkey Multiple Vulnerabilities - Advisories - Community

[SECURITY] Fedora 11 Update: nginx-0.7.64-1.fc11

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Understanding the TLS Renegotiation Attack - Educated Guesswork

IBM - Security Vulnerabilities and HIPER APARs fixed in DB2 for Linux, UNIX, and Windows Version 9.1 Fix Pack 9

Red Hat update for java-1.6.0-ibm - Advisories - Community

'[security bulletin] HPSBUX02517 SSRT100058 rev.1 - HP-UX Running OpenSSL, Remote Unauthorized Inform' - MARC

Red Hat Customer Portal

HP Systems Insight Manager Multiple Vulnerabilities - Advisories - Community

The Slackware Linux Project: Slackware Security Advisories

Multiple Vendor TLS Protocol Session Renegotiation Security Vulnerability

Repository / Oval Repository

Fedora update for openssl - Advisories - Community

Repository / Oval Repository

USN-927-4: nss vulnerability | Ubuntu

Red Hat Customer Portal

Red Hat Customer Portal

SecurityTracker.com Archives - Cisco Wireless Control System Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-th

Red Hat Customer Portal - Access to 24x7 support and knowledge

SecurityTracker.com Archives - Cisco Digital Media Media Player and Digital Media Manager Protocol Flaw in SSL Renegotiation May Let Re

Debian update for nss - Advisories - Community

Red Hat Customer Portal

404 Not Found

Pony Mail!

rhn.redhat.com | Red Hat Support

'[security bulletin] HPSBMA02534 SSRT090180 rev.1 - HP System Management Homepage (SMH) for Linux and' - MARC

APPLE-SA-2010-05-18-2 Java for Mac OS X 10.5 Update 7

Citrix Secure Gateway TLS Session Renegotiation Plaintext Injection - Secunia Advisories - Vulnerability Information - Secunia.com

404 Not Found

404 Not Found

Debian update for openssl - Advisories - Community

SOL10737 - SSL Renegotiation vulnerability - CVE-2009-3555 / VU#120541

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:008

Repository / Oval Repository

CVE-2011-4745, CVE-2011-4746, CVE-2011-4747, CVE-2009-3555, CVE-2011-4748, CVE-2011-4749, XSS, Cross Site Scripting in psa v10.

URL shortener analytics and visitor tracking | clicky.me

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM PM12247: SHIP APAR FIXES FOR H28W610 FIX PACK 6.1.0.31. - United States

Avaya Products TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Gentoo Linux Documentation -- IcedTea JDK: Multiple vulnerabilities

oss-security - CVEs for nginx

1021653

Red Hat Customer Portal

Red Hat JBoss Enterprise Web Server Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-in-the-Middle Attacks - SecurityT

Repository / Oval Repository

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:019

rhn.redhat.com | Red Hat Support

rhn.redhat.com | Red Hat Support

65202

Zeus Web Server Multiple Vulnerabilities - Advisories - Community

Red Hat Customer Portal

VMSA-2010-0019.3

Red Hat Knowledgebase: Is Red Hat affected by TLS renegotiation MITM attacks (CVE-2009-3555)?

'OpenSSL 0.9.8l released' - MARC

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Cisco Security Advisory: Transport Layer Security Renegotiation Vulnerability - Cisco Systems

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

'[security bulletin] HPSBUX02524 SSRT100089 rev.1 - HP-UX Running Java, Remote Execution of Arbitrary' - MARC

oss-security - CVE-2009-3555 for TLS renegotiation MITM attacks

Re: TLS renegotiation MITM

Avaya Products NSS TLS Session Renegotiation Vulnerability - Advisories - Community

Aruba Mobility Controller TLS Session Renegotiation Plaintext Injection - Advisories - Community

Debian -- Security Information -- DSA-2141-1 openssl

Full Disclosure: Re: SSL/TLS MiTM PoC

IBM X-Force Exchange

IBM WebSphere Application Server for z/OS Multiple Vulnerabilities - Advisories - Community

SecurityTracker.com Archives - Content Services Switch Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Mid

SecurityTracker.com Archives - Solaris Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-in-the-Middle Attacks

Support

About Secunia Research | Flexera

access.redhat.com | CVE-2009-3555

G-SEC - Blog: TLS / SSLv3 renegotiation vulnerability explained (Update #2)(

'CVE-2009-3555 - apache/mod_ssl vulnerability and mitigation' - MARC

USN-923-1: OpenJDK vulnerabilities | Ubuntu

#273029: Security Vulnerability in the Transport Layer Security (TLS) and Secure Sockets Layer 3.0 (SSLv3) Protocols Involving Handshake R

Red Hat update for gnutls - Advisories - Community

Red Hat Customer Portal

ASA-2010-308 (RHSA-2010-0768)

About Secunia Research | Flexera

Pony Mail!

Fedora update for tomcat-native - Advisories - Community

IBM MS81: WebSphere MQ Internet Pass-Thru - United States

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Cisco Wide Area Application Services Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Ma

SecurityTracker.com Archives - Sun Java System Web Server Protocol Flaw in SSL Renegotiation Lets Remote Users Conduct Man-in-the-Mi

Red Hat Customer Portal

VMware vCenter / ESX Server Update for Oracle (Sun) JRE - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Cisco NX-OS Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle Attacks

Oracle Critical Patch Update Pre-Release Announcement - October 2010

Red Hat Customer Portal

[SECURITY] Fedora 10 Update: httpd-2.2.14-1.fc10

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Advisories | Mandriva

ASA-2010-307 (RHSA-2010-0770)

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:013

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat Customer Portal

IBM - IBM HTTP Server interim fix for PM00675

APPLE-SA-2010-05-18-1 Java for Mac OS X 10.6 Update 2

IBM IC68055: SECURITY: TRANSPORT LAYER SECURITY (TLS) HANDSHAKE RENEGOTIATION WEAK SECURITY CVE-2009-3555 - U

Advisory: TLS protocol vulnerable to Man In The Middle attack - Opera Knowledge Base

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Ubuntu update for openjdk - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Cisco Firewall Services Module Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-t

SecurityTracker.com Archives - Cisco ONS Protocol Flaw in SSL Renegotiation May Let Remote Users Conduct Man-in-the-Middle Attacks

USN-927-1: NSS vulnerability | Ubuntu

OpenSSL TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

F5 Products TLS Session Renegotiation Plaintext Injection Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

'[security bulletin] HPSBOV02762 SSRT100825 rev.1 - HP Secure Web Server (SWS) for OpenVMS running CS' - MARC

OpenBSD 4.6 errata

Repository / Oval Repository

rhn.redhat.com | Red Hat Support

Mozilla Thunderbird Multiple Vulnerabilities - Advisories - Community

Support | Red Hat

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

oss-security - Re: CVE-2009-3555 for TLS renegotiation MITM attacks

Red Hat Customer Portal

The Apache Tomcat Native - Miscellaneous Documentation -

Release notice for Ingate Firewall® 4.8.1 and Ingate SIParator® 4.8.1

60972

Apache Mail Archives

#274990: Security Vulnerability in the Transport Layer Security (TLS) and Secure Sockets Layer 3.0 (SSLv3) Protocols Affects Multiple Serve

SecurityFocus

Page not found - Thủ thuật nhà cái

VMware vCenter Server 4.1 Update 1 Release Notes

US-CERT Vulnerability Note VU#120541

Red Hat Customer Portal

SecurityTracker.com Archives - Sun GlassFish Enterprise Server/Sun Java Application Server SSL Renegotiation Lets Remote Users Conduc

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

HPSBUX02482 SSRT090249 rev.2 - HP-UX Running OpenSSL, Remote Unauthorized Data Injection, Denial of Service (DoS) - c01945686 -

CVE Program record

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-11-20	Tomas Hoger	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com

Legacy QID Mappings

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

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

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

997471 Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-f7w7-6pjc-wwm6)