CVE-2015-4000

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-4000
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-21 00:59:00 UTC
Updated	2023-02-09 16:15:00 UTC
Description	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not pro

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	-	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Application	Google	Chrome	-	All	All	All
Application	Google	Chrome	-	All	All	All
Operating System	Hp	Hp-ux	b.11.31	All	All	All
Operating System	Hp	Hp-ux	b.11.31	All	All	All
Application	Ibm	Content Manager	8.5	All	All	All
Application	Ibm	Content Manager	8.5	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
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	-	All	All	All
Application	Mozilla	Firefox	39.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	39.0	All	All	All
Application	Mozilla	Firefox Esr	31.8	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	31.8	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Operating System	Mozilla	Firefox Os	2.2	All	All	All
Operating System	Mozilla	Firefox Os	2.2	All	All	All
Application	Mozilla	Network Security Services	3.19	All	All	All
Application	Mozilla	Network Security Services	3.19	All	All	All
Application	Mozilla	Seamonkey	2.35	All	All	All
Application	Mozilla	Seamonkey	2.35	All	All	All
Application	Mozilla	Thunderbird	31.8	All	All	All
Application	Mozilla	Thunderbird	38.1	All	All	All
Application	Mozilla	Thunderbird	31.8	All	All	All
Application	Mozilla	Thunderbird	38.1	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Opera	Opera Browser	-	All	All	All
Application	Opera	Opera Browser	-	All	All	All
Application	Oracle	Jdk	1.6.0	update95	All	All
Application	Oracle	Jdk	1.6.0	update_95	All	All

Application	Oracle	Jdk	1.7.0	update75	All	All
Application	Oracle	Jdk	1.7.0	update80	All	All
Application	Oracle	Jdk	1.7.0	update_80	All	All
Application	Oracle	Jdk	1.8.0	update45	All	All
Application	Oracle	Jdk	1.8.0	update_33	All	All
Application	Oracle	Jdk	1.6.0	update_95	All	All
Application	Oracle	Jdk	1.7.0	update75	All	All
Application	Oracle	Jdk	1.7.0	update_80	All	All
Application	Oracle	Jdk	1.8.0	update45	All	All
Application	Oracle	Jdk	1.8.0	update_33	All	All
Application	Oracle	Jre	1.6.0	update_95	All	All
Application	Oracle	Jre	1.7.0	update_75	All	All
Application	Oracle	Jre	1.7.0	update_80	All	All
Application	Oracle	Jre	1.8.0	update_33	All	All
Application	Oracle	Jre	1.8.0	update_45	All	All
Application	Oracle	Jre	1.6.0	update_95	All	All
Application	Oracle	Jre	1.7.0	update_75	All	All
Application	Oracle	Jre	1.7.0	update_80	All	All
Application	Oracle	Jre	1.8.0	update_33	All	All
Application	Oracle	Jre	1.8.0	update_45	All	All
Application	Oracle	Jrockit	r28.3.6	All	All	All
Application	Oracle	Jrockit	r28.3.6	All	All	All
Application	Oracle	Sparc-opl Service Processor	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All

References

Reference
HP Network Node Manager iTLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker
IBM Tivoli Monitoring TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] SUSE-SU-2015:1320-1: important: Security update for

IBM Tivoli Storage Manager FastBack for Workstations TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Conn

Oracle Critical Patch Update Advisory - April 2016

IBM SPSS Analytic Server TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] openSUSE-SU-2015:1229-1: important: Security update

HP IceWall TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005 - Apple Support

'[security bulletin] HPSBGN03404 rev.1 - HP Service Health Reporter, Remote Unauthorized Modification' - MARC

Red Hat Customer Portal

FortiGuard

IBM Rational Quality Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

'[security bulletin] HPSBGN03362 rev.1 - HP Discovery and Dependency Mapping Inventory (DDMI) with TL' - MARC

NetBSD-SA2015-008

'[security bulletin] HPSBMU03401 rev.1 - HP Operations Manager for UNIX and Linux, Remote Unauthorize' - MARC

Document Display | HPE Support Center

APPLE-SA-2015-06-30-1 iOS 8.4

[security-announce] SUSE-SU-2016:0224-1: important: Security update for

'[security bulletin] HPSBGN03407 rev.1 - HP Operations Manager for Windows, Remote Unauthorized Modif' - MARC

IBM Rational ClearQuest TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] openSUSE-SU-2016:0255-1: important: Security update

IBM Lotus Notes and Domino TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

[security-announce] openSUSE-SU-2015:1288-1: important: Security update

Red Hat Customer Portal

Document Display | HPE Support Center

Official HP® Support

IBM Flex System Manager SMIA Configuration Tool TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connec

IBM Rational Rhapsody Design Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Sec

Oracle Critical Patch Update - July 2016

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM WebSphere MQ Telemetry (CVE-2015-4000) - United States

'[security bulletin] HPSBGN03533 rev.1 - HP Enterprise Cloud Service Automation and Codar, Remote Una' - MARC

'[security bulletin] HPSBGN03361 rev.1 - HP UCMDB, HP UCMDB Configuration Manager, HP UCMDB Browser, ' - MARC

IBM Rational Software Architect TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTrac

Debian -- Security Information -- DSA-3300-1 iceweasel

IBM WebSphere MQ Telemetry TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTrack

IBM Security Bulletin:Vulnerability in Diffie-Hellman ciphers affects Rational Build Forge (CVE-2015-4000) - United States

Juniper Networks - 2016-04 Security Bulletin: Junos Space: Multiple privilege escalation vulnerabilities in Junos Space (CVE-2016-1265) - Kn

'[security bulletin] HPSBGN03351 rev.1 - HP IceWall SSO Dfw, SSO Certd, MCRP, and Federation Agent ru' - MARC

IBM Security Bulletin: Vulnerabilities in OpenSSL including Logjam affect IBM Tivoli Netcool System Service Monitors/Application Service Mor

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM® WebSphere Real Time (CVE-2015-4000)

HP integrated Lights Out (iLO) TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

Logjam, FREAK and Upcoming Changes in OpenSSL - OpenSSL Blog

IBM Support

Red Hat Customer Portal

IBM notice: The page you requested cannot be displayed

Oracle Critical Patch Update - October 2015

IBM Rational ClearCase TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

IBM AIX Sendmail TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Red Hat Customer Portal

OpenSSL: Multiple vulnerabilities (GLSA 201506-02) — Gentoo security

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Security Network Protection (CVE-2015-4000)

Debian -- Security Information -- DSA-3339-1 openjdk-6

[SECURITY] Fedora 21 Update: nss-3.19.1-1.0.fc21

Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM® DB2® LUW (CVE-2015-4000) - United States

CVE-2015-4000 - Citrix Security Advisory for DHE_EXPORT TLS Vulnerability

Oracle Critical Patch Update - July 2015

HPE 支援文件 - HPE 支援中心

openssl.org/news/secadv/20150611.txt

Document Display | HPE Support Center

[security-announce] SUSE-SU-2015:1268-1: important: Security update for

Red Hat Customer Portal

Document Display | HPE Support Center

IBM DB2 TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

USN-2656-2: Firefox vulnerabilities | Ubuntu

'[security bulletin] HPSBGN03402 rev.2 - HP Performance Manager, Remote Disclosure of Information' - MARC

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Tivoli Composite Application Manager for Transactions (CVE-2015-40

[security-announce] SUSE-SU-2015:1185-1: important: Security update for

Document Display | HPE Support Center

[security-announce] openSUSE-SU-2016:0261-1: important: Security update

IBM SPSS Modeler TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

IBM SPSS Modeler TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox

RHSA-2016:2056

[security-announce] SUSE-SU-2015:1183-1: important: Security update for

aix.software.ibm.com/aix/efixes/security/sendmail_advisory2.asc

Oracle Secure Global Desktop TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

openSUSE-SU-2016:0483-1: moderate: Security update for socat

'[security bulletin] HPSBUX03363 rev.1 - HP-UX Apache Web Server running OpenSSL, Remote Disclosure o' - MARC

IBM WebSphere Application Server Community Edition TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Con

APPLE-SA-2015-06-30-2 OS X Yosemite v10.10.4 and Security Update 2015-005

IBM Tivoli Netcool System Service Monitor TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Se

Apache TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[SECURITY] Fedora 22 Update: nss-3.19.1-1.0.fc22

USN-2673-1: Thunderbird vulnerabilities | Ubuntu

Red Hat Customer Portal

Red Hat Customer Portal

Lotus Quickr for WebSphere Portal TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityT

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction

'[security bulletin] HPSBGN03373 rev.1 - HP Release Control running TLS, Remote Disclosure of Informa' - MARC

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Tivoli Monitoring (CVE-2015-4000) - United States

IBM AIX TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Red Hat Customer Portal

NSS 3.19.1 release notes - Mozilla | MDN

Red Hat Customer Portal

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Rational ClearCase (CVE-2015-4000) - United States

Red Hat Customer Portal

Broadcom Support Portal

NSS accepts export-length DHE keys with regular DHE cipher suites — Mozilla

Weak Diffie-Hellman and the Logjam Attack

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Cognos Metrics Manager (CVE-2015-4000) - United States

IBM The Diffie-Hellman vulnerability known as Logjam in Apache Tomcat may affect IBM WebSphere Application Server Community Edition (

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects multiple IBM Rational products based on IBM Jazz technology (CVE-2015-

[security-announce] SUSE-SU-2015:1269-1: important: Security update for

'[security bulletin] HPSBGN03399 rev.1 - HP BSM Connector (BSMC), Remote Unauthorized Modification, D' - MARC

Apple OS X TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

'[security bulletin] HPSBUX03512 SSRT102254 rev.1 - HP-UX Web Server Suite running Apache, Remote Den' - MARC

[security-announce] SUSE-SU-2015:1143-1: important: Security update for

Document Display | HPE Support Center

HP Release Control TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Debian -- Security Information -- DSA-3688-1 nss

HPE Service Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

'[security bulletin] HPSBGN03411 rev.1 - HP Operations Agent Virtual Appliance, Remote Unauthorized D' - MARC

'[security bulletin] HPSBUX03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Infor' - MARC

Document Display | HPE Support Center

Red Hat Customer Portal

Document Display | HPE Support Center

[security-announce] SUSE-SU-2015:1319-1: important: Security update for

Red Hat Customer Portal

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects FileNet Content Manager, IBM Content Foundation and FileNet BPM (CVE-201

HP Operations Manager for Linux and UNIX TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - S

Red Hat Customer Portal

USN-2696-1: OpenJDK 7 vulnerabilities | Ubuntu

Debian -- Security Information -- DSA-3316-1 openjdk-7

[security-announce] SUSE-SU-2015:1581-1: important: Security update for

OpenSSL TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Oracle Solaris Third Party Bulletin - July 2015

Oracle Communications Messaging Server TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Se

Document Display | HPE Support Center

IBM Tivoli Composite Application Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Se

IBM Security Network Protection TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTrac

'[security bulletin] HPSBGN03405 rev.1 - HP Integration Adaptor, Remote Unauthorized Modification, Di' - MARC

IBM Rational Build Forge TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Cognos Mobile app on Android (CVE-2015-4000) - United States

NetBSD TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

About the security content of iOS 8.4 - Apple Support

StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center

HP Support document - HP Support Center

Red Hat Customer Portal

Mozilla Network Security Service (NSS): Multiple vulnerabilities (GLSA 201701-46) — Gentoo security

Debian -- Security Information -- DSA-3324-1 icedove

IBM notice: The page you requested cannot be displayed

Document Display | HPE Support Center

IBM WebSphere Real Time TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM WebSphere MQ Internet Passthru (CVE-2015-4000)

www.openssl.org/news/secadv_20150611.txt

HP Performance Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] SUSE-SU-2015:1449-1: important: Security update for

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

Document Display | HPE Support Center

FortiGuard

IBM WebSphere MQIPT TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

openSUSE-SU-2015:1684-1: moderate: Security update for apache2

HPE integrated Lights Out (iLO) TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTrac

Juniper Junos TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Document Display | HPE Support Center

HP Discovery & Dependency Mapping Inventory TLS RC4 Algorithm Lets Remote Users Decrypt Data - SecurityTracker

[security-announce] SUSE-SU-2015:1182-1: important: Security update for

HP Operations Manager for Windows TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Security

CVE-2015-4000 Diffie-Hellman Export Cipher Suite vulnerability in Multiple NetApp Products | NetApp Product Security

[security-announce] openSUSE-SU-2016:0226-1: important: Security update

USN-2656-1: Firefox vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2015:1184-1: important: Security update for

Logjam: the latest TLS vulnerability explained

SSL/TLS LogJam Man in the Middle Security Bypass Vulnerability

Red Hat Customer Portal

Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security

2015-05 Out of Cycle Security Bulletin: "Logjam" passive attack on sub-1024 DH groups, and active downgrade attack of TLS to DHE_EXPOR

IBM Infosphere Optim Query Workload Tuner for DB2 TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Conn

[security-announce] openSUSE-SU-2015:1277-1: important: Security update

[security-announce] openSUSE-SU-2015:1289-1: important: Security update

[security-announce] SUSE-SU-2015:1177-1: important: Security update for

[security-announce] SUSE-SU-2015:1150-1: important: Security update for

Debian -- Security Information -- DSA-3287-1 openssl

IBM Cognos Mobile App TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

CVE-2015-4000 - Logjam TLS Vulnerability | Puppet

IBM License Metric Tool TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Rational ClearQuest(CVE-2015-4000)

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects IBM Rational ClearQuest(CVE-2015-4000)

[SECURITY] Fedora 20 Update: nss-3.19.1-1.0.fc20

IBM InfoSphere Guardium TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

USN-2706-1: OpenJDK 6 vulnerabilities | Ubuntu

Security Bulletin: Multiple vulnerabilities in IBM Java Runtime affect IBM Rational Software Architect , Rational Software Architect for Websphe

McAfee Firewall Enterprise TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

McAfee KnowledgeBase - Intel Security - Security Bulletin: Seven OpenSSL CVEs Announced on June 11, 2015

Red Hat Customer Portal

Oracle Java SE Multiple Flaws Lets Local and Remote Users Gain Elevated Privileges and Remote Users Partially Access Data, Modify Data,

IBM Rational Team Concert TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracker

[security-announce] SUSE-SU-2016:0262-1: important: Security update for

Security Bulletin: Multiple vulnerabilities in IBM Java SDK affect IBM SPSS Modeler (CVE-2015-4000, CVE-2015-0478, CVE-2015-0488)

[security-announce] SUSE-SU-2015:1181-1: important: Security update for

[security-announce] SUSE-SU-2015:1663-1: important: Security update for

Document Display | HPE Support Center

CVE-2015-4000

'[security bulletin] HPSBMU03356 rev.1 - HP Business Service Automation Essentials (BSAE) running TLS' - MARC

openSUSE-SU-2016:0478-1: moderate: Security update for socat

IBM FileNet Content Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

'[security bulletin] HPSBMU03345 rev.1 - HP Network Node Manager i (NNMi) and Smart Plugins (iSPIs) f' - MARC

openSUSE-SU-2015:1209-1: moderate: Security update for mysql-community-s

IBM Content Manager Enterprise Edition TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - Secu

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects Tivoli Storage Manager FastBack for Workstations (CVE-2015-4000)

IBM Cognos Metrics Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections - SecurityTracke

Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Security F

SolarWinds Storage Manager Release Notes

IBM Rational Software Architect Design Manager TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connectio

oss-security - CVE-2015-4000 - TLS does not properly convey server's ciphersuite choice

Oracle Critical Patch Update Advisory - January 2021

Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201603-11) — Gentoo Security

weakdh.org/imperfect-forward-secrecy.pdf

IBM Security Bulletin: Vulnerability in Diffie-Helman ciphers affects IBM License Metric Tool and IBM Endpoint Manager for Software Use Ana

1138554 – (CVE-2015-4000) NSS accepts export-length DHE keys with regular DHE cipher suites ("Logjam")

Oracle Solaris Bulletin - January 2016

IBM Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects Content Manager Enterprise Edition (CVE-2015-4000) - United States

[security-announce] openSUSE-SU-2015:1139-1: important: Security update

Oracle Critical Patch Update - January 2016
HP Project and Portfolio Management Center TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections -
Document Display | HPE Support Center
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

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

591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

671073 EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2643)

671109 EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2509)

710518 Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201701-46)

753736 SUSE Enterprise Linux Security Update for nrpe (SUSE-SU-2023:0586-1)