CVE-2014-3566

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-3566
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-15 00:55:00 UTC
Updated	2023-09-12 14:55:00 UTC
Description	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which r

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	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
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All

Application	Ibm	Vios	2.2.0.10	All	All	All
Application	Ibm	Vios	2.2.0.11	All	All	All
Application	Ibm	Vios	2.2.0.12	All	All	All
Application	Ibm	Vios	2.2.0.13	All	All	All
Application	Ibm	Vios	2.2.1.0	All	All	All
Application	Ibm	Vios	2.2.1.1	All	All	All
Application	Ibm	Vios	2.2.1.3	All	All	All
Application	Ibm	Vios	2.2.1.4	All	All	All
Application	Ibm	Vios	2.2.1.5	All	All	All
Application	Ibm	Vios	2.2.1.6	All	All	All
Application	Ibm	Vios	2.2.1.7	All	All	All
Application	Ibm	Vios	2.2.1.8	All	All	All
Application	Ibm	Vios	2.2.1.9	All	All	All
Application	Ibm	Vios	2.2.2.0	All	All	All
Application	Ibm	Vios	2.2.2.1	All	All	All
Application	Ibm	Vios	2.2.2.2	All	All	All
Application	Ibm	Vios	2.2.2.3	All	All	All
Application	Ibm	Vios	2.2.2.4	All	All	All
Application	Ibm	Vios	2.2.2.5	All	All	All
Application	Ibm	Vios	2.2.3.0	All	All	All
Application	Ibm	Vios	2.2.3.1	All	All	All
Application	Ibm	Vios	2.2.3.2	All	All	All
Application	Ibm	Vios	2.2.3.3	All	All	All
Application	Ibm	Vios	2.2.3.4	All	All	All
Operating System	Ibm	Vios	2.2.0.10	All	All	All
Operating System	Ibm	Vios	2.2.0.11	All	All	All
Operating System	Ibm	Vios	2.2.0.12	All	All	All
Operating System	Ibm	Vios	2.2.0.13	All	All	All
Operating System	Ibm	Vios	2.2.1.0	All	All	All
Operating System	Ibm	Vios	2.2.1.1	All	All	All
Operating System	Ibm	Vios	2.2.1.3	All	All	All
Operating System	Ibm	Vios	2.2.1.4	All	All	All
Operating System	Ibm	Vios	2.2.1.5	All	All	All
Operating System	Ibm	Vios	2.2.1.6	All	All	All
Operating System	Ibm	Vios	2.2.1.7	All	All	All

Operating System	Ibm	Vios	2.2.1.8	All	All	All
Operating System	Ibm	Vios	2.2.1.9	All	All	All
Operating System	Ibm	Vios	2.2.2.0	All	All	All
Operating System	Ibm	Vios	2.2.2.1	All	All	All
Operating System	Ibm	Vios	2.2.2.2	All	All	All
Operating System	Ibm	Vios	2.2.2.3	All	All	All
Operating System	Ibm	Vios	2.2.2.4	All	All	All
Operating System	Ibm	Vios	2.2.2.5	All	All	All
Operating System	Ibm	Vios	2.2.3.0	All	All	All
Operating System	Ibm	Vios	2.2.3.1	All	All	All
Operating System	Ibm	Vios	2.2.3.2	All	All	All
Operating System	Ibm	Vios	2.2.3.3	All	All	All
Operating System	Ibm	Vios	2.2.3.4	All	All	All
Operating System	Ibm	Vios	2.2.0.10	All	All	All
Operating System	Ibm	Vios	2.2.0.11	All	All	All
Operating System	Ibm	Vios	2.2.0.12	All	All	All
Operating System	Ibm	Vios	2.2.0.13	All	All	All
Operating System	Ibm	Vios	2.2.1.0	All	All	All
Operating System	Ibm	Vios	2.2.1.1	All	All	All
Operating System	Ibm	Vios	2.2.1.3	All	All	All
Operating System	Ibm	Vios	2.2.1.4	All	All	All
Operating System	Ibm	Vios	2.2.1.5	All	All	All
Operating System	Ibm	Vios	2.2.1.6	All	All	All
Operating System	Ibm	Vios	2.2.1.7	All	All	All
Operating System	Ibm	Vios	2.2.1.8	All	All	All
Operating System	Ibm	Vios	2.2.1.9	All	All	All
Operating System	Ibm	Vios	2.2.2.0	All	All	All
Operating System	Ibm	Vios	2.2.2.1	All	All	All
Operating System	Ibm	Vios	2.2.2.2	All	All	All
Operating System	Ibm	Vios	2.2.2.3	All	All	All
Operating System	Ibm	Vios	2.2.2.4	All	All	All
Operating System	Ibm	Vios	2.2.2.5	All	All	All
Operating System	Ibm	Vios	2.2.3.0	All	All	All
Operating System	Ibm	Vios	2.2.3.1	All	All	All
Operating System	Ibm	Vios	2.2.3.2	All	All	All

Operating System	Ibm	Vios	2.2.3.3	All	All	All
Operating System	Ibm	Vios	2.2.3.4	All	All	All
Operating System	Mageia	Mageia	3.0	All	All	All
Operating System	Mageia	Mageia	4.0	All	All	All
Operating System	Mageia	Mageia	3.0	All	All	All
Operating System	Mageia	Mageia	4.0	All	All	All
Operating System	Netbsd	Netbsd	5.1	All	All	All
Operating System	Netbsd	Netbsd	5.1.1	All	All	All
Operating System	Netbsd	Netbsd	5.1.2	All	All	All
Operating System	Netbsd	Netbsd	5.1.3	All	All	All
Operating System	Netbsd	Netbsd	5.1.4	All	All	All
Operating System	Netbsd	Netbsd	5.2	All	All	All
Operating System	Netbsd	Netbsd	5.2.1	All	All	All
Operating System	Netbsd	Netbsd	5.2.2	All	All	All
Operating System	Netbsd	Netbsd	6.0	All	All	All
Operating System	Netbsd	Netbsd	6.0	beta	All	All
Operating System	Netbsd	Netbsd	6.0.1	All	All	All
Operating System	Netbsd	Netbsd	6.0.2	All	All	All
Operating System	Netbsd	Netbsd	6.0.3	All	All	All
Operating System	Netbsd	Netbsd	6.0.4	All	All	All
Operating System	Netbsd	Netbsd	6.0.5	All	All	All
Operating System	Netbsd	Netbsd	6.0.6	All	All	All
Operating System	Netbsd	Netbsd	6.1	All	All	All
Operating System	Netbsd	Netbsd	6.1.1	All	All	All
Operating System	Netbsd	Netbsd	6.1.2	All	All	All
Operating System	Netbsd	Netbsd	6.1.3	All	All	All
Operating System	Netbsd	Netbsd	6.1.4	All	All	All
Operating System	Netbsd	Netbsd	6.1.5	All	All	All
Operating System	Netbsd	Netbsd	5.1	All	All	All
Operating System	Netbsd	Netbsd	5.1.1	All	All	All
Operating System	Netbsd	Netbsd	5.1.2	All	All	All
Operating System	Netbsd	Netbsd	5.1.3	All	All	All
Operating System	Netbsd	Netbsd	5.1.4	All	All	All
Operating System	Netbsd	Netbsd	5.2	All	All	All
Operating System	Netbsd	Netbsd	5.2.1	All	All	All
Operating System	Netbsd	Netbsd	5.2.2	All	All	All

Operating System	Netbsd	Netbsd	6.0	All	All	All
Operating System	Netbsd	Netbsd	6.0	beta	All	All
Operating System	Netbsd	Netbsd	6.0.1	All	All	All
Operating System	Netbsd	Netbsd	6.0.2	All	All	All
Operating System	Netbsd	Netbsd	6.0.3	All	All	All
Operating System	Netbsd	Netbsd	6.0.4	All	All	All
Operating System	Netbsd	Netbsd	6.0.5	All	All	All
Operating System	Netbsd	Netbsd	6.0.6	All	All	All
Operating System	Netbsd	Netbsd	6.1	All	All	All
Operating System	Netbsd	Netbsd	6.1.1	All	All	All
Operating System	Netbsd	Netbsd	6.1.2	All	All	All
Operating System	Netbsd	Netbsd	6.1.3	All	All	All
Operating System	Netbsd	Netbsd	6.1.4	All	All	All
Operating System	Netbsd	Netbsd	6.1.5	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	9.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	10.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	9.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	All	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Application	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All

Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All
Application	Openssl	Openssl	0.9.8y	All	All	All
Application	Openssl	Openssl	0.9.8z	All	All	All
Application	Openssl	Openssl	0.9.8za	All	All	All
Application	Openssl	Openssl	0.9.8zb	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All

Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All

Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All
Application	Openssl	Openssl	0.9.8y	All	All	All
Application	Openssl	Openssl	0.9.8z	All	All	All
Application	Openssl	Openssl	0.9.8za	All	All	All
Application	Openssl	Openssl	0.9.8zb	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	All	All	All
Application	Openssl	Openssl	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All

Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Application	Oracle	Database	11.2.0.4	All	All	All
Application	Oracle	Database	12.1.0.2	All	All	All
Application	Oracle	Database	11.2.0.4	All	All	All
Application	Oracle	Database	12.1.0.2	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	5.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	7.0	All	All	All

References

Reference
SSL 3.0 Protocol Vulnerability and POODLE Attack | US-CERT
Oracle Solaris Bulletin - April 2016
'[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC
Oracle Critical Patch Update Advisory - April 2016
Cisco CSS 11500 Series Content Security Switch SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracke
Red Hat Customer Portal
McAfee KnowledgeBase - McAfee Security Bulletin - Three SSLv3 Vulnerabilities
Oracle Bulletin Board Update - January 2015
Red Hat Customer Portal - Access to 24x7 support and knowledge
'[security bulletin] HPSBMU03267 rev.1 - HP Matrix Operating Environment and HP CloudSystem Matrix ru' - MARC
[security-announce] SUSE-SU-2014:1526-1: important: Security update for
Debian -- Security Information -- DSA-3147-1 openjdk-6
About Secunia Research | Flexera

About Secunia Research | Flexera

Red Hat Customer Portal

About Secunia Research | Flexera

'[security bulletin] HPSBMU03263 rev.3 - HP Insight Control running OpenSSL, Remote Disclosure of Inf' - MARC

Mageia Advisory: MGASA-2014-0416 - Updated openssl packages fix security vulnerabilities

The POODLE Attack and the End of SSL 3.0 | Mozilla Security Blog

Red Hat Customer Portal

HP Support document - HP Support Center

Red Hat Customer Portal

Cisco Intrusion Prevention System SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

About Secunia Research | Flexera

Cisco AnyConnect Secure Mobility Client SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

'[security bulletin] HPSBMU03184 rev.1 - HP SiteScope running SSL, Remote Disclosure of Information' - MARC

Support / Security / Advisories / / MDVSA-2014:203 | Mandriva

'[security bulletin] HPSBGN03192 rev.1 - HP Remote Device Access: Instant Customer Access Server (iCA' - MARC

About the security content of Xcode 7.0 - Apple Support

Oracle Critical Patch Update - July 2016

Red Hat Customer Portal

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

Red Hat Customer Portal

'[security bulletin] HPSBGN03208 rev.1 - HP Cloud Service Automation running SSLv3, Remote Disclosure' - MARC

POODLE: SSLv3 Vulnerability - Lenovo Support (US)

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

'[security bulletin] HPSBST03195 rev.1 - HP 3PAR Service Processor (SP) running OpenSSL and Bash, Rem' - MARC

Security Advisory-SSLv3 POODLE Vulnerability in Huawei Products - Huawei PSIRT

HPE Support document - HPE Support Center

HPE Support document - HPE Support Center

Cisco Prime Security Manager SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Google Online Security Blog: This POODLE bites: exploiting the SSL 3.0 fallback

Cisco Wireless LAN Controller SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

access.redhat.com | CVE-2014-3566

OpenSSL CVE-2014-3566 Man In The Middle Information Disclosure Vulnerability

Red Hat Customer Portal

Pony Mail!

'[security bulletin] HPSBGN03254 rev.1 - HP Service Health Analyzer running SSLv3, Remote Disclosure ' - MARC

Red Hat Customer Portal

Red Hat Customer Portal

About the security content of OS X Yosemite v10.10 - Apple Support

Microsoft Windows SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Arista - Security Advisory 0007

'[security bulletin] HPSBMU03294 rev.1 - HP Process Automation running OpenSSL, Remote Disclosure of ' - MARC

Vulnerabilities resolved in TRITON APX Version 8.0

Google Groups

USN-2486-1: OpenJDK 6 vulnerabilities | Ubuntu

Blue Coat Director SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

'[security bulletin] HPSBMU03183 rev.2 - HP Server Automation and Server Automation Virtual Appliance' - MARC

SecurityFocus

'[security bulletin] HPSBGN03205 rev.1 - HP Insight Remote Support Clients running SSLv3, Remote Disc' - MARC

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

'[security bulletin] HPSBGN03201 rev.1 - HP Asset Manager running SSLv3, Remote Disclosure of Informa' - MARC

1076983 – (POODLE) Padding oracle attack on SSL 3.0

'[security bulletin] HPSBMU03221 rev.1 - HP Connect-IT running SSLv3, Remote Disclosure of Informatio' - MARC

'[security bulletin] HPSBMU03214 rev.1 - HP Systinet running SSLv3, Remote Disclosure of Information' - MARC

SecurityFocus

'[security bulletin] HPSBMU03283 rev.1 - HP Virtual Connect Enterprise Manager SDK running OpenSSL on' - MARC

'[security bulletin] HPSBGN03252 rev.1 - HP AppPulse Active running SSLv3, Remote Disclosure of Infor' - MARC

Oracle Critical Patch Update - July 2015

About Secunia Research | Flexera

GitHub - mpgn/poodle-PoC: Poodle (Padding Oracle On Downgraded Legacy Encryption) attack

Red Hat Customer Portal

'[security bulletin] HPSBST03418 rev.1 - HP P6000 Command View Software, Remote Disclosure of Informa' - MARC

Philips Intellispace Portal ISP Vulnerabilities | ICS-CERT

'[security bulletin] HPSBGN03233 rev.1 - HP OneView running OpenSSL, Remote Denial of Service (DoS), ' - MARC

APPLE-SA-2015-09-16-2 Xcode 7.0

[security-announce] SUSE-SU-2015:0578-1: important: Security update for

'[security bulletin] HPSBST03265 rev.1 - HP VMA SAN Gateway running Bash Shell and OpenSSL, Remote De' - MARC

[SECURITY] Fedora 21 Update: fossil-1.33-1.fc21

'[security bulletin] HPSBMU03241 rev.1 - HP Network Automation running SSLv3, Remote Disclosure of In' - MARC

Node v0.10.33 (Stable)

Red Hat Customer Portal

About Security Update 2014-005 - Apple Support

About the security content of Apple TV 7.0.1 - Apple Support

Multiple vulnerabilities in OpenSSL (Third Party Vulnerability Resolution Blog)

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

POODLE: SSLv3 Vulnerability - US

Pony Mail!

Cisco Nexus SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

'[security bulletin] HPSBMU03259 rev.1 - HP Version Control Repository Manager running OpenSSL on Lin' - MARC

www.openssl.org/news/secadv_20141015.txt

Citrix NetScaler SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

[security-announce] SUSE-SU-2015:0344-1: important: Security update for

TippingPoint Intrusion Prevention System Local Security Manager SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic

Pony Mail!

IBM Security Bulletin: - United States

'[security bulletin] HPSBPI03107 rev.1 - HP LaserJet Printers and MFPs, HP OfficeJet Printers and MFP' - MARC

'[security bulletin] HPSBMU03223 rev.1 - HP Insight Control server provisioning running SSLv3, Remote' - MARC

'[security bulletin] HPSBUX03273 SSRT101951 rev.1 - HP-UX running Java6, Remote Unauthorized Access, ' - MARC

Logstash 1.4.3 released | Elastic

CVE-2014-3566 SSL v3.0 Nondeterministic CBC Padding Vulnerability in Multiple NetApp Products | NetApp Product Security

SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability

'[security bulletin] HPSBGN03164 rev.1 - HP IceWall SSO Dfw, SSO Certd and MCRP running OpenSSL, Remo' - MARC

Red Hat Customer Portal

HPE Support document - HPE Support Center

Red Hat Customer Portal

VMSA-2015-0003.15 | United States

Red Hat Customer Portal

'[security bulletin] HPSBGN03222 rev.1 - HP Enterprise Maps running SSLv3, Remote Disclosure of Infor' - MARC

Red Hat Customer Portal

docs.ipswitch.com/MOVEit/DMZ82/ReleaseNotes/MOVEitReleaseNotes82.pdf

About the security content of OS X Yosemite v10.10.2 and Security Update 2015-001 - Apple Support

'[security bulletin] HPSBGN03209 rev.1 - HP Application Lifecycle Management running SSLv3, Remote Di' - MARC

Microsoft Security Advisory 3009008

Red Hat Customer Portal

Oracle Solaris Third Party Bulletin - October 2015

[security-announce] SUSE-SU-2016:1457-1: important: Security update for

[security-announce] SUSE-SU-2015:0376-1: important: Security update for

USN-2487-1: OpenJDK 7 vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2014:1361-1: important: Security update for

Pony Mail!

Red Hat Customer Portal

NEOHAPSIS - Peace of Mind Through Integrity and Insight

About the security content of OS X Server v2.2.5 - Apple Support

CVE-2014-3566 in Ubuntu

'[security bulletin] HPSBMU03262 rev.1 - HP Version Control Agent running OpenSSL on Linux and Window' - MARC

Oracle Critical Patch Update - January 2015

[security-announce] SUSE-SU-2015:0392-1: important: Security update for

About the security content of OS X Server v3.2.2 - Apple Support

'[security bulletin] HPSBMU03259 rev.1 - HP Version Control Repository Manager running OpenSSL on Lin' - MARC

'[security bulletin] HPSBMU03234 rev.1 - HP Vertica Analytics Platform running SSLv3, Remote Disclosu' - MARC

'[security bulletin] HPSBUX03194 rev.1 - HP-UX running sendmail(1M), Remote Disclosure of Information' - MARC

Security Advisory 3009008 updated - MSRC - Site Home - TechNet Blogs

How POODLE Happened — Indistinguishable from Random

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

Cisco TelePresence SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Red Hat Customer Portal

About Secunia Research | Flexera

'[security bulletin] HPSBMU03152 rev.1 - HP Operations Orchestration running SSL, Remote Disclosure o' - MARC

Citrix XenMobile Device Manager SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

lists.apache.org/thread.html/rec7160382badd3ef4ad017a22f64a266c7188b9ba71394f0...

Document Display | HPE Support Center

AST-2014-011

Citrix Security Advisory for CVE-2014-3566 - SSLv3 Protocol Flaw

NEOHAPSIS - Peace of Mind Through Integrity and Insight

Google Groups

NetBSD-SA2014-015

CDH Issues

IBM Update: Security Bulletin: Vulnerability in SSLv3 affects IBM® SDK, Java Technology Edition for AIX/VIOS (CVE-2014-3566) - United Sta

[security-announce] SUSE-SU-2016:1459-1: important: Security update for

security - How do I patch/workaround SSLv3 POODLE vulnerability (CVE-2014-3566)? - Ask Ubuntu

[security-announce] openSUSE-SU-2015:0190-1: important: Security update

Oracle Solaris Third Party Bulletin - July 2015

A Few Thoughts on Cryptographic Engineering: Attack of the week: POODLE

Red Hat Customer Portal

'[security bulletin] HPSBMU03416 rev.1 - HP Data Protector, Remote Disclosure of Information' - MARC

Red Hat Customer Portal

Support / Security / Advisories / / MDVSA-2015:062 | Mandriva

'[security bulletin] HPSBGN03202 rev.1 - HP CMS: Configuration Manager running OpenSSL, Remote Disclo' - MARC

'[security bulletin] HPSBGN03391 rev.1 - HP Universal CMDB Foundation, Discovery, Configuration Manag' - MARC

About Secunia Research | Flexera

IBM Security Bulletin: Vulnerability in SSLv3 affects Directory Server (CVE-2014-3566) - United States

McAfee KnowledgeBase - McAfee Security Bulletin - ePO update fixes multiple Oracle Java vulnerabilities

OpenSSL SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Red Hat Customer Portal

CVE-2014-3566: Removing SSLv3 from BIG-IP

lists.apache.org/thread.html/rfb87e0bf3995e7d560afeed750fac9329ff5f1ad49da3651...

Debian -- Security Information -- DSA-3144-1 openjdk-7

About Secunia Research | Flexera

About Secunia Research | Flexera

'[security bulletin] HPSBGN03253 rev.1 - HP Business Process Insight (BPI) running SSLv3, Remote Disc' - MARC

Debian -- Security Information -- DSA-3489-1 lighttpd

Pony Mail!

Security Bulletin: Multiple vulnerabilities in IBM Java Runtime affect Content Manager Enterprise Edition (CVE-2014-3566, CVE-2014-6457, C

'[security bulletin] HPSBGN03332 rev.1 - HP Operations Analytics running SSLv3, Remote Denial of Serv' - MARC

'[security bulletin] HPSBGN03203 rev.1 - HP CMS: UCMDB Browser running OpenSSL, Remote Disclosure of ' - MARC

Red Hat Customer Portal

Red Hat Customer Portal

About Secunia Research | Flexera

'Patch to mitigate CVE-2014-3566 ("POODLE")' - MARC

IBM Security Bulletin: A security vulnerability has been identified in IBM Tivoli Directory Server shipped with AIX/VIOS (CVE-2014-3566) - Unit

Red Hat Customer Portal

IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States

'[security bulletin] HPSBUX03281 SSRT101968 rev.1 - HP-UX running Java7, Remote Unauthorized Access, ' - MARC

Support | The POODLE weakness in the SSL protocol (CVE-2014-3566)

[security-announce] openSUSE-SU-2014:1331-1: important: update for opens

Red Hat Customer Portal

About the security content of iOS 8.1 - Apple Support

'[security bulletin] HPSBOV03227 rev.1 - HP SSL for OpenVMS, Remote Disclosure of Information, Denial' - MARC

[SECURITY] Fedora 19 Update: openssl-1.0.1e-40.fc19

Pony Mail!

[SECURITY] Fedora 21 Update: openssl-1.0.1j-1.fc21

[security-announce] SUSE-SU-2015:0345-1: important: Security update for

[security-announce] SUSE-SU-2014:1357-1: important: Security update for

About Secunia Research | Flexera

Citrix Secure Gateway SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Bug 1152789 – CVE-2014-3566 SSL/TLS: Padding Oracle On Downgraded Legacy Encryption attack

www.openssl.org/~bodo/ssl-poodle.pdf

SecurityFocus

Pony Mail!

[security-announce] SUSE-SU-2014:1549-1: important: Security update for

Cisco Unified Communications Manager SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

About Secunia Research | Flexera

'[security bulletin] HPSBGN03305 rev.1 - HP Business Service Management (BSM) products running SSLv3,' - MARC

Pony Mail!

HP Operations Orchestration SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Cisco IOS SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Red Hat Customer Portal

Cisco Application Control Engine SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201507-14) — Gentoo Security

About Secunia Research | Flexera

[SECURITY] Fedora 20 Update: openssl-1.0.1e-40.fc20

'[security bulletin] HPSBMU03304 rev.1 - HP Insight Control server deployment on Linux and Windows, R' - MARC

Oracle Critical Patch Update - April 2015

Red Hat Customer Portal

Red Hat Customer Portal

About the security content of OS X Server v4.0 - Apple Support

POODLE: SSLv3 vulnerability (CVE-2014-3566) - Red Hat Customer Portal

[SECURITY] Fedora 22 Update: fossil-1.33-1.fc22

[security-announce] openSUSE-SU-2016:0640-1: important: Security update

Red Hat Customer Portal

'[security bulletin] HPSBGN03191 rev.1 - HP Remote Device Access: Virtual Customer Access System (vCA' - MARC

Home | Blue Coat Systems, Inc.

Blue Coat PacketShaper SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

'[security bulletin] HPSBGN03251 rev.1 - HP Storage Essentials running SSLv3, Remote Disclosure of In' - MARC

aix.software.ibm.com/aix/efixes/security/openssl_advisory11.asc

Red Hat Customer Portal

Document Display | HPE Support Center

CVE-2014-3566 - POODLE SSLv3 Vulnerability | Puppet

[security-announce] SUSE-SU-2015:0503-1: important: Security update for

Red Hat Customer Portal

IBM SDK, Java Technology Edition fixes to mitigate against the POODLE security vulnerability (CVE-2014-3566) - United States

About Secunia Research | Flexera

'[security bulletin] HPSBMU03301 rev.1 - HP BladeSystem c-Class Onboard Administrator running OpenSSL' - MARC

Red Hat Customer Portal

'[security bulletin] HPSBHF03275 rev.1 - HP Integrated Lights-Out 2, 3, and 4 (iLO 2, iLO 3, iLO 4), ' - MARC

About Secunia Research | Flexera

APPLE-SA-2015-01-27-4 OS X 10.10.2 and Security Update 2015-001

'[security bulletin] HPSBUX03162 SSRT101767 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

'[security bulletin] HPSBHF03300 rev.1 - HP Network Products running OpenSSL, Remote Denial of Servic' - MARC

Red Hat Customer Portal

McAfee KnowledgeBase - McAfee Security Bulletin - POODLE Vulnerability

Oracle Solaris Third Party Bulletin - April 2015

ImperialViolet - POODLE attacks on SSLv3

Red Hat Customer Portal

IBM Security Bulletin: Vulnerability in SSLv3 affects IBM HTTP Server (CVE-2014-3566) - United States

'[security bulletin] HPSBHF03156 rev.1 - HP TippingPoint Intrusion Prevention System (IPS) Local Secu' - MARC

Pony Mail!

About Secunia Research | Flexera

'[security bulletin] HPSBPI03360 rev.2 - HP LaserJet Printers and MFPs, HP OfficeJet Printers and MFP' - MARC

'[security bulletin] HPSBMU03260 rev.1 - HP System Management Homepage running OpenSSL on Linux and W' - MARC

Oracle Critical Patch Update - July 2017

Red Hat Customer Portal

Cisco ASA SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

Blue Coat ProxySG SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker

'[security bulletin] HPSBGN03255 rev.1 - HP OpenCall Media Platform (OCMP) running SSLv3, Remote Deni' - MARC

Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView

'[security bulletin] HPSBGN03569 rev.1 - HPE OneView for VMware vCenter (OV4VC), Remote Disclosure of' - MARC

Pony Mail!

'[security bulletin] HPSBGN03237 rev.1 - HP Insight Remote Support v7 Clients running SSLv3, Remote D' - MARC

About Secunia Research | Flexera

[security-announce] SUSE-SU-2015:0336-1: important: Security update for
'[security bulletin] HPSBMU03261 rev.2 - HP Systems Insight Manager running OpenSSL on Linux and Wind' - MARC
Debian -- Security Information -- DSA-3053-1 openssl
Red Hat Customer Portal
Oracle Solaris Bulletin - January 2016
Cisco Email Security Appliance SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker
About Secunia Research | Flexera
Vulnerability Note VU#577193 - POODLE vulnerability in SSL 3.0
claws-mail: Multiple Vulnerabilities (GLSA 201606-11) — Gentoo security
IBM Tivoli Directory Server SSL 3.0 Protocol Downgrade Flaw Lets Remote Users Decrypt SSL Traffic - SecurityTracker
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)

590349 Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

590888 Phoenix Contact Innominate mGuard Secure Sockets Layer (SSL) protocol 3.0 Security Vulnerability (20141022_001)

590920 ABB Relion 650 series Secure Sockets Layer (SSL) 3.0 Protocol and POODLE Attack Multiple Vulnerabilities (ABB-VU-PSAC-1MRG018009)

591002 ABB ETL600 series POODLE Attack and Secure Sockets Layer (SSL) 3.0 Protocol Vulnerability (ABB-VU-PSAC-1KHW028571)

591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)

591350 General Electric D20MX Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (PRSN-0006)

591378 ABB RTU500 series Secure Sockets Layer (SSL) 3.0 Protocol and POODLE Attack in the webserver component Vulnerability (ABB-VU-PSAC-1KGT090264)

591388 ABB AFx series Secure Sockets Layer (SSL) 3.0 Protocol and POODLE Attack Vulnerability (ABB-VU-PSAC- 1KHW028569)

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

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