CVE-2015-3405

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3405
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-09 16:29:00 UTC
Updated	2023-02-13 00:49:00 UTC
Description	ntp-keygen in ntp 4.2.8px before 4.2.8p2-RC2 and 4.3.x before 4.3.12 does not generate MD5 keys with sufficient entropy c

Risk And Classification

Problem Types: CWE-331

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	21	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All
Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All

Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.9	All	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All
Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All
Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.9	All	All	All
Operating System	Opensuse	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Opensuse	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Opensuse Project	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Opensuse Project	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui 6	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui 6	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11.0	sp3	All	All

References

Reference	Source	Link
Bug 2797 – ntp-keygen trapped in endless loop for MD5 keys on big-endian machines	CONFIRM	bugs.ntp.o
access.redhat.com | CVE-2015-3405	MISC	access.red
[SECURITY] Fedora 21 Update: ntp-4.2.6p5-30.fc21	FEDORA	lists.fedora
Red Hat Customer Portal	REDHAT	rhn.redhat.
Debian -- Security Information -- DSA-3388-1 ntp	DEBIAN	www.debia
[security-announce] SUSE-SU-2015:1173-1: important: Security update for	SUSE	lists.opens
Red Hat Customer Portal	REDHAT	rhn.redhat.
Document Display | HPE Support Center	CONFIRM	support.hp
All diffs for ChangeSet 1.3308.4.1	CONFIRM	bk1.ntp.org
Bug 1210324 – CVE-2015-3405 ntp: ntp-keygen may generate non-random symmetric keys on big-endian systems	CONFIRM	bugzilla.red
Red Hat Customer Portal	MISC	access.red
oss-security - Re: CVE request: ntp-keygen may generate non-random symmetric keys on big-endian systems	MLIST	www.openv
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle
Red Hat Customer Portal	MISC	access.red
NTP 'ntp-keygen.c' Predictable Random Number Generator Weakness	BID	www.secur
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	www.oracle
Debian -- Security Information -- DSA-3223-1 ntp	DEBIAN	www.debia
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

43837 HPE Comware 5 And Comware 7 Switches And Routers using NTP, Remote Denial Of Service (HPESBHF03886)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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