CVE-2015-5300

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-5300
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-21 14:29:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The panic_gate check in NTP before 4.2.8p5 is only re-enabled after the first change to the system clock that was greater tl

Risk And Classification

Problem Types: CWE-361

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	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	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	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	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Ntp	Ntp	All	p4	All	All

Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	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 Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	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 Eus	6.7.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	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
Application	Suse	Linux Enterprise Debuginfo	11	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All

Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Manager	2.1	All	All	All
Operating System	Suse	Manager	2.1	All	All	All
Operating System	Suse	Manager Proxy	2.1	All	All	All
Operating System	Suse	Manager Proxy	2.1	All	All	All
Operating System	Suse	Openstack Cloud	5	All	All	All
Operating System	Suse	Openstack Cloud	5	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
Red Hat Customer Portal
support.ntp.org/bin/view/Main/SecurityNotice
FreeBSD-SA-16:02
USN-2783-1: NTP vulnerabilities | Ubuntu
Oracle Critical Patch Update - July 2016
Citrix XenServer Multiple Security Updates
[security-announce] SUSE-SU-2016:1247-1: important: Security update for
October 2015 Network Time Protocol Daemon (ntpd) Vulnerabilities in Multiple NetApp Products | NetApp Product Security
Debian -- Security Information -- DSA-3388-1 ntp
Security Bulletin: IBM Security Access Manager for Mobile is affected by NTP vulnerabilities (CVE-2015-5300, CVE-2015-7704, CVE-2015-81

ntpd Flaw Lets Remote Users Modify Time on the Target ntp Service in Certain Cases - SecurityTracker
openSUSE-SU-2016:1423-1: moderate: Security update for ntp
1271076 – (CVE-2015-5300) CVE-2015-5300 ntp: MITM attacker can force ntpd to make a step larger than the panic threshold
Security Bulletin: Real-time compression appliance (CVE-2015-5300 CVE-2015-7704 CVE-2015-8138)
Security Bulletin: IBM Flex System Manager (FSM) is affected by multiple ntp vulnerabilities
[security-announce] SUSE-SU-2016:1912-1: important: Security update for
Security Bulletin: Vulnerabilities in NTP affect IBM Security Network Protection (CVE-2015-5300, CVE-2015-7704, and CVE-2015-8138)
[SECURITY] Fedora 23 Update: ntp-4.2.6p5-34.fc23
Bugtraq: [slackware-security] ntp (SSA:2016-054-04)
[security-announce] SUSE-SU-2016:2094-1: important: Security update for
Network Time Protocol CVE-2015-5300 Man in the Middle Security Bypass Vulnerability
[security-announce] SUSE-SU-2016:1311-1: important: Security update for
Security Bulletin: Multiple vulnerabilities in ntp affect PowerKVM
support.ntp.org/bin/view/Main/NtpBug2956
IBM Support
SA113: January 2016 NTP Security Vulnerabilities | Blue Coat Systems, Inc.
Siemens RUGGEDCOM ROX-based Devices NTP Vulnerabilities | ICS-CERT
Attacking the Network Time Protocol
[security-announce] openSUSE-SU-2016:1292-1: important: Security update
[security-announce] SUSE-SU-2016:1175-1: important: Security update for
aix.software.ibm.com/aix/efixes/security/ntp_advisory5.asc
Security Bulletin: Multiple vulnerabilities in Network Time Protocol(NTP) affect WebSphere DataPower XC10 Appliance (CVE-2016-5300, CVE
[SECURITY] Fedora 21 Update: ntp-4.2.6p5-34.fc21
Oracle Solaris Bulletin - January 2016
[security-announce] SUSE-SU-2016:1177-1: important: Security update for
Oracle Linux Bulletin - October 2015
[SECURITY] Fedora 22 Update: ntp-4.2.6p5-36.fc22
Security Bulletin: IBM Security Access Manager for Web is affected by NTP vulnerabilities (CVE-2015-5300, CVE-2015-7704, CVE-2015-8138
Security Bulletin: Vulnerabilities in ntp affect Power Hardware Management Console (CVE-2015-5300, CVE-2015-7704, CVE-2015-8138)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.