CVE-2015-7705

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-7705
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 20:29:00 UTC
Updated	2021-11-17 22:15:00 UTC
Description	The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified imp

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	-	All	All
Application	Citrix	Xenserver	6.5	-	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	-	All	All
Application	Citrix	Xenserver	6.5	-	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Ntp	Ntp	All	All	All	All

Application	Ntp	Ntp	4.2.8	-	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta2	All	All
Application	Ntp	Ntp	4.2.8	p1-beta3	All	All
Application	Ntp	Ntp	4.2.8	p1-beta4	All	All
Application	Ntp	Ntp	4.2.8	p1-beta5	All	All
Application	Ntp	Ntp	4.2.8	p1-rc1	All	All
Application	Ntp	Ntp	4.2.8	p1-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.2.8	p2-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3-rc1	All	All
Application	Ntp	Ntp	4.2.8	p3-rc2	All	All
Application	Ntp	Ntp	4.2.8	p3-rc3	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	-	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta2	All	All
Application	Ntp	Ntp	4.2.8	p1-beta3	All	All
Application	Ntp	Ntp	4.2.8	p1-beta4	All	All
Application	Ntp	Ntp	4.2.8	p1-beta5	All	All
Application	Ntp	Ntp	4.2.8	p1-rc1	All	All
Application	Ntp	Ntp	4.2.8	p1-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.2.8	p2-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3-rc1	All	All
Application	Ntp	Ntp	4.2.8	p3-rc2	All	All
Application	Ntp	Ntp	4.2.8	p3-rc3	All	All

Hardware	Siemens	Tim 4r-ie	-	All	All	All
Hardware	Siemens	Tim 4r-ie Dnp3	-	All	All	All
Operating System	Siemens	Tim 4r-ie Dnp3 Firmware	All	All	All	All
Operating System	Siemens	Tim 4r-ie Firmware	All	All	All	All

References

Reference
[security-announce] openSUSE-SU-2016:1329-1: important: Security update for ntp - openSUSE Security Announce - openSUSE Mailing List
Network Time Protocol CVE-2015-7705 Denial of Service Vulnerability
[security-announce] SUSE-SU-2016:1247-1: important: Security update for
USN-2783-1: NTP vulnerabilities | Ubuntu
Siemens SIMATIC NET CP 443-1 OPC UA | CISA
[security-announce] SUSE-SU-2016:1568-1: important: Security update for
Arista - Security Advisory 0016
Citrix XenServer Multiple Security Updates
SecurityFocus
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security
SecurityFocus
October 2015 Network Time Protocol Daemon (ntpd) Vulnerabilities in Multiple NetApp Products | NetApp Product Security
cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf
openSUSE-SU-2016:1423-1: moderate: Security update for ntp
openSUSE-SU-2015:2016-1: moderate: Security update for ntp
Broadcom Support Portal
Siemens TIM 4R-IE Devices | CISA
eprint.iacr.org/2015/1020.pdf
support.ntp.org/bin/view/Main/NtpBug2901
SecurityFocus
ntp Multiple Flaws Let Remote Users Deny Service, View Files, and Bypass Authentication to Modify the Time - SecurityTracker
[security-announce] SUSE-SU-2016:1471-1: important: Security update for
[security-announce] SUSE-SU-2016:1311-1: important: Security update for
Vulnerability Note VU#718152 - NTP.org ntpd contains multiple vulnerabilities
SecurityFocus
[security-announce] SUSE-SU-2016:1278-1: important: Security update for ntp - openSUSE Security Announce - openSUSE Mailing Lists
[security-announce] SUSE-SU-2016:1912-1: important: Security update for
Slackware Security Advisory - ntp Updates ≈ Packet Storm
[security-announce] SUSE-SU-2016:1291-1: important: Security update for ntp - openSUSE Security Announce - openSUSE Mailing Lists

[security-announce] SUSE-SU-2016:2094-1: important: Security update for
1274184 – (CVE-2015-7705) CVE-2015-7705 ntp: denial of service by trigerring rate limiting on NTP server
Attacking the Network Time Protocol
support.ntp.org/bin/view/Main/SecurityNotice
Document Display | HPE Support Center
cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf
Multiple Vulnerabilities in ntpd Affecting Cisco Products - October 2015
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

590721 Siemens TIM 4R-IE Devices Multiple Vulnerabilities (ICSA-21-103-11)

590736 Siemens SIMATIC NET CP 443-1 OPC UA Multiple Vulnerabilities (ICSA-21-159-11)