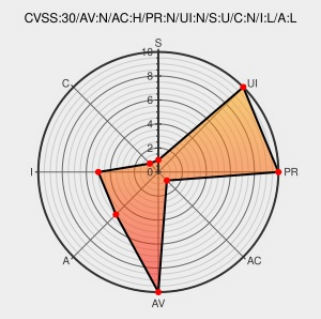
CVE-2015-8140

Published on: 01/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-8140

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ntp from Ntp contain the following vulnerability:

The ntpq protocol in NTP before 4.2.8p7 allows remote attackers to conduct replay attacks by sniffing the network.

CVE-2015-8140 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	LOW

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2016:1247-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:1247
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo	Third Party Advisory	GENTOO GLSA-201607-15

Security	security.gentoo.org text/html	
openSUSE-SU-2016:1423-1: moderate: Security update for ntp	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1423
[security-announce] SUSE-SU-2016:1311-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:1311
Vulnerability Note VU#718152 - NTP.org ntpd contains multiple vulnerabilities	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#718152
No Description Provided	Vendor Advisory support.ntp.org text/html	CONFIRM support.ntp.org/bin/view/Main/NtpBug2947
January 2020 NTP Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200204-0003/
ntp Multiple Flaws Let Remote Users Spoof Messages, Obtain Potentially Sensitive Information, and Deny Service - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034782
SA113: January 2016 NTP Security Vulnerabilities | Blue Coat Systems, Inc.	Third Party Advisory bto.bluecoat.com text/html	CONFIRM bto.bluecoat.com/security-advisory/sa113
	security.FreeBSD.org text/plain	FREEBSD FreeBSD-SA-16:09
[security-announce] SUSE-SU-2016:1177-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:1177
[security-announce] openSUSE-SU-2016:1292-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1292
Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products - January 2016	Third Party Advisory tools.cisco.com text/html	CISCO 20160120 Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products - January 2016
[security-announce] SUSE-SU-2016:1175-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:1175

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntp	Ntp	All	p6	All	All

cpe:2.3:a:ntp:ntp:*:p6:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→