CVE-2016-4954

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-4954
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-05 01:59:00 UTC
Updated	2023-11-07 02:32:00 UTC
Description	The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of s

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	4.2.8	p4	All	All
Application	Ntp	Ntp	4.2.8	p5	All	All
Application	Ntp	Ntp	4.2.8	p6	All	All
Application	Ntp	Ntp	4.2.8	p7	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	4.2.8	p4	All	All
Application	Ntp	Ntp	4.2.8	p5	All	All
Application	Ntp	Ntp	4.2.8	p6	All	All
Application	Ntp	Ntp	4.2.8	p7	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	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All

Hardware	Siemens	Simatic Net Cp 443-1 Opc Ua	-	All	All	All
Operating System	Siemens	Simatic Net Cp 443-1 Opc Ua Firmware	All	All	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
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	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	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
Application	Suse	Manager	2.1	All	All	All
Application	Suse	Manager	2.1	All	All	All
Application	Suse	Manager Proxy	2.1	All	All	All
Application	Suse	Manager Proxy	2.1	All	All	All
Application	Suse	Openstack Cloud	5	All	All	All
Application	Suse	Openstack Cloud	5	All	All	All

References

Reference	Source	Link
Oracle Solaris Bulletin - April 2016	CONFIRM	www.oracle.com
Document Display | HPE Support Center	CONFIRM	h20566.www2.hpe.c
SecurityFocus	BUGTRAQ	www.securityfocus.c
support.ntp.org/bin/view/Main/NtpBug3044	CONFIRM	support.ntp.org
[security-announce] openSUSE-SU-2016:1636-1: important: Security update	SUSE	lists.opensuse.org
Siemens SIMATIC NET CP 443-1 OPC UA | CISA	MISC	us-cert.cisa.gov
[security-announce] openSUSE-SU-2016:1583-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:1568-1: important: Security update for	SUSE	lists.opensuse.org
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security	GENTOO	security.gentoo.org
Vulnerability Note VU#321640 - NTP.org ntpd is vulnerable to denial of service and other vulnerabilities	CERT-VN	www.kb.cert.org
[security-announce] SUSE-SU-2016:1602-1: important: Security update for	SUSE	lists.opensuse.org

cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf	CONFIRM	cert-portal.siemens.c
SecurityFocus	BUGTRAQ	www.securityfocus.c
[SECURITY] Fedora 23 Update: ntp-4.2.6p5-41.fc23 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
SecurityFocus	BUGTRAQ	www.securityfocus.c
[SECURITY] Fedora 23 Update: ntp-4.2.6p5-41.fc23 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
ntp Multiple Bugs Let Remote Users Modify Parameters and Deny Service - SecurityTracker	SECTRACK	www.securitytracker.
support.ntp.org/bin/view/Main/SecurityNotice	CONFIRM	support.ntp.org
Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products: June 2016	CISCO	tools.cisco.com
SecurityFocus	BUGTRAQ	www.securityfocus.c
Vulnerability Note VU#321640 - NTP.org ntpd is vulnerable to denial of service and other vulnerabilities	CERT-VN	www.kb.cert.org
Slackware Security Advisory - ntp Updates ≈ Packet Storm	MISC	packetstormsecurity.
[security-announce] SUSE-SU-2016:1563-1: important: Security update for	SUSE	lists.opensuse.org
[SECURITY] Fedora 24 Update: ntp-4.2.6p5-41.fc24 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 22 Update: ntp-4.2.6p5-41.fc22 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Bug 3044 – Processing spoofed server packets	CONFIRM	bugs.ntp.org
SecurityFocus	BUGTRAQ	www.securityfocus.c
[SECURITY] Fedora 22 Update: ntp-4.2.6p5-41.fc22 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[security-announce] SUSE-SU-2016:1912-1: important: Security update for	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:2094-1: important: Security update for	SUSE	lists.opensuse.org
SecurityFocus	BUGTRAQ	www.securityfocus.c
Siemens TIM 4R-IE Devices | CISA	CONFIRM	us-cert.cisa.gov
FreeBSD Security Advisory - FreeBSD-SA-16:24.ntp ≈ Packet Storm	MISC	packetstormsecurity.
[security-announce] SUSE-SU-2016:1584-1: important: Security update for	SUSE	lists.opensuse.org
FreeBSD-SA-16:24	FREEBSD	security.FreeBSD.org
[SECURITY] Fedora 24 Update: ntp-4.2.6p5-41.fc24 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf	CONFIRM	cert-portal.siemens.c
USN-3096-1: NTP vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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)

690292 Free Berkeley Software Distribution (FreeBSD) Security Update for FreeBSD (7cfcea05-600a-11e6-a6c3-14dae9d210b8)