



CVE-2014-9294

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-9294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-20 02:59:00 UTC
Updated	2021-11-17 22:15:00 UTC
Description	util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attacker

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

Red Hat Customer Portal
Bug 1176035 – CVE-2014-9294 ntp: ntp-keygen uses weak random number generator and seed when generating MD5 keys
Bug 2666 – non-cryptographic random number generator with weak seed
'[security bulletin] HPSBPV03266 rev.1 - Certain HP Networking and H3C Switches and Routers running N' - MARC
Oracle Critical Patch Update - October 2016
support.ntp.org/bin/view/Main/SecurityNotice
Document Display HPE Support Center
HPE Support document - HPE Support Center
Changes for util/ntp-keygen.c
McAfee KnowledgeBase - McAfee Security Bulletin - Firewall Enterprise update fixes NTP vulnerabilities
'[security bulletin] HPSBOV03505 rev.1 - TCP/IP Services for OpenVMS running NTP, Remote Code Executi' - MARC
Vulnerability Note VU#852879 - Network Time Protocol (NTP) Project NTP daemon (ntpd) contains multiple vulnerabilities
NTP 'ntp-keygen.c' Predictable Random Number Generator Weakness

Security Advisory SA62209 - Cisco ACNS (Application and Content Networking System) NTP Multiple Buffer Overflow Vulnerabilities - Secuni
Red Hat Customer Portal
'[security bulletin] HPSBGN03277 rev.1 - HP Virtualization Performance Viewer, Remote Execution of Co' - MARC
Support / Security / Advisories / / MDVSA-2015:003 Mandriva
Multiple Vulnerabilities in ntpd Affecting Cisco Products
Arista - Security Advisory 0008
'[security bulletin] HPSBUX03240 SSRT101872 rev.2 - HP-UX Running NTP, Remote Execution of Code, Deni' - MARC
Mageia Advisory: MGASA-2014-0541 - Updated ntp packages fix security vulnerabilities
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
591117 Siemens SINUMERIK Controllers Multiple Vulnerabilities (SSA-749212)

© [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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)