



CVE-2009-0021

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

Summary

CVE	CVE-2009-0021
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-07 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	NTP 4.2.4 before 4.2.4p5 and 4.2.5 before 4.2.5p150 does not properly check the return value from the OpenSSL EVP_VerifyFinal() function, which could allow an attacker to bypass the authentication process and execute arbitrary code with root privileges.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntp	Ntp	4.2.0	All	All	All

Application	Ntp	Ntp	4.2.2	All	All	All
Application	Ntp	Ntp	4.2.4p1	All	All	All
Application	Ntp	Ntp	4.2.4p2	All	All	All
Application	Ntp	Ntp	4.2.4p3	All	All	All
Application	Ntp	Ntp	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References	
Reference	Source
Slackware update for ntp - Secunia.com	af854a3a-212
Support	af854a3a-212
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:005	af854a3a-212
SecurityFocus	af854a3a-212
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	af854a3a-212
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	af854a3a-212
oCERT.org - oCERT Advisories	af854a3a-212
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-212
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
The Slackware Linux Project: Slackware Security Advisories	af854a3a-212
Red Hat update for ntp - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-212
Webmail- OVH	af854a3a-212
NTP Signature Validation Flaw Lets Remote Users Bypass Validation Checks - SecurityTracker	af854a3a-212
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
[ntp:announce] NTP 4.2.4p6 Released	af854a3a-212
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:008	af854a3a-212
NTP OpenSSL "EVP_VerifyFinal()" Spoofing Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-212
Repository / Oval Repository	af854a3a-212
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	af854a3a-212
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#)