



# CVE-2004-2761

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-2761
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-01-05 20:30:00 UTC
<b>Updated</b>	2018-10-19 15:30:00 UTC
<b>Description</b>	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conc

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">letf</a>	MD5	-	All	All	All
Application	<a href="#">letf</a>	MD5	-	All	All	All
Application	<a href="#">letf</a>	X.509 Certificate	-	All	All	All
Application	<a href="#">letf</a>	X.509 Certificate	-	All	All	All

## References

Reference	Source
Document Display   HPE Support Center	CON
USN-740-1: NSS vulnerability   Ubuntu	UBU
Security Vulnerability Research & Defense : Information regarding MD5 collisions problem	MISC
Document Display   HPE Support Center	CON
Bug 648886 – CVE-2004-2761 MD5: MD5 Message-Digest Algorithm is not collision resistant	CON
Red Hat Customer Portal	RED
[SECURITY] Fedora 9 Update: nss-3.12.2.0-2.fc9	FED
Philips Intellispace Portal ISP Vulnerabilities   ICS-CERT	MISC
Your request has been blocked. This could be due to several reasons.	MISC
Creating a rogue CA certificate	MISC

MD5 Considered Harmful Today: Creating a rogue CA certificate - SecurityReason.com	SRE
MD5 Weaknesses Could Lead to Certificate Forgery at Mozilla Security Blog	MISC
SecurityFocus	BUG
SecurityTracker.com Archives - Red Hat Certificate System Bugs Let Remote Users Obtain One-Time PINs and Generate Certificates	SEC
Page not found   Dan Kaminsky's Blog	MISC
www.win.tue.nl/hashclash/SoftIntCodeSign	MISC
Red Hat Certificate Server MD5 and SCEP Vulnerabilities - Advisories - Community	SEC
Document Display   HPE Support Center	CON
IETF RFC 3279 X.509 Certificate MD5 Signature Collision Vulnerability	BID
About Secunia Research   Flexera	SEC
Fedora update for nss - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
Tim Callan's SSL Blog - Online Security	MISC
www.win.tue.nl/hashclash/rogue-ca	MISC
US-CERT Vulnerability Note VU#836068	CER
Cisco Security Response: MD5 Hashes May Allow for Certificate Spoofing [Products & Services] - Cisco Systems	CISC
Red Hat Customer Portal	RED
CVE Program record	CVE
NVD vulnerability detail	NVD

#### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-01-07	Mark J Cox	Please see <a href="http://kbase.redhat.com/faq/docs/DOC-15379">http://kbase.redhat.com/faq/docs/DOC-15379</a>

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](#).

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