CVE-2004-2761

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2004-2761
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-05 20:30:00 UTC
Updated	2018-10-19 15:30:00 UTC
Description	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	Ietf	Md5	-	All	All	All
Application	Ietf	Md5	-	All	All	All
Application	Ietf	X.509 Certificate	-	All	All	All
Application	Ietf	X.509 Certificate	-	All	All	All

References

Reference	Sour
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 http://kbase.redhat.com/faq/docs/DOC-15379

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