



CVE-2004-0758

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

Summary

CVE	CVE-2004-0758
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Mozilla 1.5 through 1.7 allows a CA certificate to be imported even when their DN is the same as that of the built-in CA root

Risk And Classification

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

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Mozilla	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	
127186 – CAN-2004-0758 Overriding built-in certificate leading to error -8182 (DoS), especially exploitable by email			af854a3a-2127-422b-9	
249004 – Importing false CA certificate leading to error -8182 (perm DoS), especially exploitable by email			af854a3a-2127-422b-9	
US-CERT Vulnerability Note VU#784278			af854a3a-2127-422b-9	
Security Announcement			af854a3a-2127-422b-9	
Gentoo Linux Documentation -- Mozilla, Firefox, Thunderbird, Galeon, Epiphany: New releases fix vulnerabilities			af854a3a-2127-422b-9	
Repository / Oval Repository			af854a3a-2127-422b-9	
ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.49/SCOSA-2005.49.txt			af854a3a-2127-422b-9	
Mozilla Security Advisory			af854a3a-2127-422b-9	
SCO OpenServer Release 5.0.7 Maintenance Pack 4 Released - Multiple Vulnerabilities Fixed			af854a3a-2127-422b-9	
redhat.com Red Hat Support			af854a3a-2127-422b-9	
Repository / Oval Repository			af854a3a-2127-422b-9	
'[FLSA-2004:2089] Updated mozilla packages fix security vulnerabilities' - MARC			af854a3a-2127-422b-9	
IBM X-Force Exchange			af854a3a-2127-422b-9	
CVE Program record			CVE.ORG	
NVD vulnerability detail			NVD	
No vendor comments have been submitted for this CVE.				
Legacy QID Mappings				
690297 Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (8d823883-0ca9-11d9-8a8a-000c41e2cdad)				