CVE-2008-2935

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

Summary

CVE	CVE-2008-2935
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-01 14:41:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple heap-based buffer overflows in the rc4 (1) encryption (aka exsltCryptoRc4EncryptFunction) and (2) decryption (aka

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlsoft	Libxslt	1.1.10	All	All	All

Application	Xmlsoft	Libxslt	1.1.11	All	All	All
Application	Xmlsoft	Libxslt	1.1.12	All	All	All
Application	Xmlsoft	Libxslt	1.1.13	All	All	All
Application	Xmlsoft	Libxslt	1.1.14	All	All	All
Application	Xmlsoft	Libxslt	1.1.15	All	All	All
Application	Xmlsoft	Libxslt	1.1.16	All	All	All
Application	Xmlsoft	Libxslt	1.1.17	All	All	All
Application	Xmlsoft	Libxslt	1.1.18	All	All	All
Application	Xmlsoft	Libxslt	1.1.19	All	All	All
Application	Xmlsoft	Libxslt	1.1.20	All	All	All
Application	Xmlsoft	Libxslt	1.1.21	All	All	All
Application	Xmlsoft	Libxslt	1.1.22	All	All	All
Application	Xmlsoft	Libxslt	1.1.23	All	All	All
Application	Xmlsoft	Libxslt	1.1.24	All	All	All
Application	Xmlsoft	Libxslt	1.1.8	All	All	All
Application	Xmlsoft	Libxslt	1.1.9	All	All	All

Vendor Declared Affected Products

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

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Debian update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SecurityFocus
www.ocert.org/patches/exslt_crypt.patch
Repository / Oval Repository
USN-633-1: libxslt vulnerabilities | Ubuntu
SecurityFocus
CXSecurity - IDS
libxslt "crypto:rc4_encrypt" and "crypto:rc4_decrypt" Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.c
Red Hat update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com
libxslt: Execution of arbitrary code — Gentoo Linux Documentation
[SECURITY] Fedora 9 Update: libxslt-1.1.24-2.fc9
Fedora update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com
504 Gateway Time-out

504 Gateway Time-out
CESA-2008-003 - rev 1
Ubuntu update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com
oCERT.org - oCERT Advisories
Support
Advisories:rPSA-2008-0306 - rPath Wiki
Debian -- Security Information -- DSA-1624-1 libxslt
SecurityFocus
Support / Security / Advisories / / MDVSA-2008:160 | Mandriva
rPath update for libxslt - Secunia.com
[SECURITY] Fedora 8 Update: libxslt-1.1.24-2.fc8
Gentoo update for libxslt - Secunia Advisories - Vulnerability Intelligence - Secunia.com
libxslt Heap Overflow in exsltCryptoRc4EncryptFunction() May Let Remote Users Execute Arbitrary Code - SecurityTracker
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**