CVE-2007-0099

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

Summary

CVE	CVE-2007-0099
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-08 20:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Race condition in the msxml3 module in Microsoft XML Core Services 3.0, as used in Internet Explorer 6 and other applicat

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-362 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	6	All	All	All

Application	Microsoft	Xml Core Services	3.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
US-CERT Technical Cyber Security Alert TA08-316A -- Microsoft Updates for Multiple Vulnerabilities	af854a3a
Microsoft Security Bulletin MS08-069 - Critical | Microsoft Docs	af854a3a
marc.info	af854a3a
archives.neohapsis.com/archives/fulldisclosure/2007-01/0113.html	af854a3a
SecurityFocus	af854a3a
InfoSec Handlers Diary Blog	af854a3a
Internet Explorer Memory Corruption Weakness - Advisories - Secunia	af854a3a
Full Disclosure: Concurrency strikes MSIE (potentially exploitable msxml3 flaws)	af854a3a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a
SecurityFocus	af854a3a
Microsoft XML Core Services Race Condition Memory Corruption Vulnerability	af854a3a
Repository / Oval Repository	af854a3a
osvdb.org/32627	af854a3a
Microsoft XML Core Services (MSXML) Bugs Let Remote Users Obtain Information and Execute Arbitrary Code - SecurityTracker	af854a3a
SecurityFocus	af854a3a
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 and Source URL Uptime Status status.cve.report