# CVE-2006-4686

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2006-4686 |
| **State** | PUBLIC |
| **Assigner** | secure@microsoft.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2006-10-10 22:07:00 UTC |
| **Updated** | 2018-10-17 21:39:00 UTC |
| **Description** | Buffer overflow in the Extensible Stylesheet Language Transformations (XSLT) processing in Microsoft XML Parser 2.6 and |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Microsoft | Xml Core Services | 3.0 | All | All | All |
| Application | Microsoft | Xml Core Services | 4.0 | All | All | All |
| Application | Microsoft | Xml Core Services | 6.0 | All | All | All |
| Application | Microsoft | Xml Core Services | 3.0 | All | All | All |
| Application | Microsoft | Xml Core Services | 4.0 | All | All | All |
| Application | Microsoft | Xml Core Services | 6.0 | All | All | All |
| Application | Microsoft | Xml Parser | 2.6 | All | All | All |
| Application | Microsoft | Xml Parser | 2.6 | All | All | All |

## References

| Reference | Source |
|---|---|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN |
| Microsoft Security Bulletin MS06-061 - Critical \| Microsoft Docs | MS |
| 29426 | OSVDB |
| Repository / Oval Repository | OVAL |
| SecurityTracker.com Archives - Microsoft XML Core Services Lets Remote Users Execute Arbitrary Code or Obtain Information | SECTRACK |
| US-CERT Vulnerability Note VU#562788 | CERT-VN |

| | |
|---|---|
| SecurityFocus | HP |
| Microsoft Windows XML Core Services XSLT Buffer Overrun Vulnerability | BID |
| Microsoft XML Core Services Information Disclosure and Code Execution - Advisories - Secunia | SECUNIA |
| 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.



**Free CVE JSON API** cve.report/api

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