



CVE-2015-2440

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-2440
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-15 00:59:00 UTC
Updated	2018-10-12 22:09:00 UTC
Description	Microsoft XML Core Services 3.0, 5.0, and 6.0 allows remote attackers to bypass the ASLR protection mechanism via a cra

Risk And Classification

Problem Types: CWE-200

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	5.0	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	5.0	All	All	All
Application	Microsoft	Xml Core Services	6.0	All	All	All

References

Reference
Microsoft XML Core Services (MSXML) Bugs Let Remote Users Obtain Potentially Sensitive Information Bypass Security Features - SecurityT Zero Day Initiative
Microsoft Security Bulletin MS15-084 - Important Microsoft Docs
76232
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)