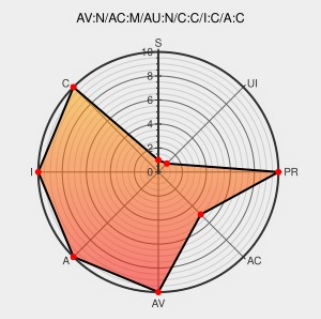
CVE-2013-1313

Published on: 02/13/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:33 PM UTC

CVE-2013-1313

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows Xp from Microsoft contain the following vulnerability:

Object Linking and Embedding (OLE) Automation in Microsoft Windows XP SP3 does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted RTF document, aka "OLE Automation Remote Code Execution Vulnerability."

CVE-2013-1313 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:16385
Microsoft Security Bulletin MS13-020 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS13-020
Microsoft Security Bulletin MS13-037 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS13-037
Microsoft Updates for Multiple Vulnerabilities | US-CERT	US Government Resource www.us-cert.gov text/html	CERT TA13-043B

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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