



# CVE-2012-0158

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

## Summary

<b>CVE</b>	CVE-2012-0158
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-04-10 21:55:00 UTC
<b>Updated</b>	2018-10-12 22:02:00 UTC
<b>Description</b>	The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Co

## Risk And Classification

**EPSS:** 0.943190000 probability, percentile 0.999510000 (date 2026-04-02)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-94

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	MSCOMCTL.OCX
<b>Name</b>	Microsoft MSCOMCTL.OCX Remote Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2012-0158">https://nvd.nist.gov/vuln/detail/CVE-2012-0158</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Biztalk Server	2002	sp1	All	All
Application	Microsoft	Biztalk Server	2002	sp1	All	All
Application	Microsoft	Commerce Server	2002	sp4	All	All
Application	Microsoft	Commerce Server	2007	sp2	All	All
Application	Microsoft	Commerce Server	2009	All	All	All
Application	Microsoft	Commerce Server	2009	r2	All	All
Application	Microsoft	Commerce Server	2002	sp4	All	All
Application	Microsoft	Commerce Server	2007	sp2	All	All

Application	Microsoft	Commerce Server	2009	All	All	All
Application	Microsoft	Commerce Server	2009	r2	All	All
Application	Microsoft	Office	2003	sp3	All	All
Application	Microsoft	Office	2007	sp2	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	All	x86	All
Application	Microsoft	Office	2010	sp1	x86	All
Application	Microsoft	Office	2003	sp3	All	All
Application	Microsoft	Office	2007	sp2	All	All
Application	Microsoft	Office	2007	sp3	All	All
Application	Microsoft	Office	2010	All	x86	All
Application	Microsoft	Office	2010	sp1	x86	All
Application	Microsoft	Office Web Components	2003	sp3	All	All
Application	Microsoft	Office Web Components	2003	sp3	All	All
Application	Microsoft	Sql Server	2000	sp4	All	All
Application	Microsoft	Sql Server	2000	sp4	analysis_services	All
Application	Microsoft	Sql Server	2005	sp4	express_advanced_services	All
Application	Microsoft	Sql Server	2005	sp4	itanium	All
Application	Microsoft	Sql Server	2005	sp4	x64	All
Application	Microsoft	Sql Server	2005	sp4	x86	All
Application	Microsoft	Sql Server	2008	r2	itanium	All
Application	Microsoft	Sql Server	2008	r2	x64	All
Application	Microsoft	Sql Server	2008	r2	x86	All
Application	Microsoft	Sql Server	2008	sp2	itanium	All
Application	Microsoft	Sql Server	2008	sp2	x64	All
Application	Microsoft	Sql Server	2008	sp2	x86	All
Application	Microsoft	Sql Server	2008	sp3	itanium	All
Application	Microsoft	Sql Server	2008	sp3	x64	All
Application	Microsoft	Sql Server	2008	sp3	x86	All
Application	Microsoft	Sql Server	2000	sp4	All	All
Application	Microsoft	Sql Server	2000	sp4	analysis_services	All
Application	Microsoft	Sql Server	2005	sp4	express_advanced_services	All
Application	Microsoft	Sql Server	2005	sp4	itanium	All
Application	Microsoft	Sql Server	2005	sp4	x64	All
Application	Microsoft	Sql Server	2005	sp4	x86	All

Application	Microsoft	Sql Server	2008	r2	itanium	All
Application	Microsoft	Sql Server	2008	r2	x64	All
Application	Microsoft	Sql Server	2008	r2	x86	All
Application	Microsoft	Sql Server	2008	sp2	itanium	All
Application	Microsoft	Sql Server	2008	sp2	x64	All
Application	Microsoft	Sql Server	2008	sp2	x86	All
Application	Microsoft	Sql Server	2008	sp3	itanium	All
Application	Microsoft	Sql Server	2008	sp3	x64	All
Application	Microsoft	Sql Server	2008	sp3	x86	All
Application	Microsoft	Visual Basic	6.0	All	runtime_extended_files	All
Application	Microsoft	Visual Basic	6.0	All	runtime_extended_files	All
Application	Microsoft	Visual Foxpro	8.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp2	All	All
Application	Microsoft	Visual Foxpro	8.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp2	All	All

## References

### Reference

[IBM X-Force Exchange](#)

[Microsoft Visual Basic Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Microsoft Commerce Server Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Microsoft SQL Server Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Repository / Oval Repository](#)

[Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability](#)

[Comment on The curious case of a CVE-2012-0158 exploit by Chris Pierce | OSINT](#)

[Microsoft Office Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Microsoft Visual FoxPro Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Microsoft Security Bulletin MS12-027 - Critical | Microsoft Docs](#)

[Microsoft BizTalk Server Windows Common Controls \(MSCOMCTL.OCX\) Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[US-CERT Alert TA12-101A -- Microsoft Updates for Multiple Vulnerabilities](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)

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](#)**