- Norton
- Small & Medium Business
- **Enterprise**
- Partners

Symantec.

- Products & Solutions

- Support & Communities

- Security Response

- Try & Buy

1. /
2. Security Response/
3. Microsoft Windows Media Center CVE-2015-2509 Remote Code Execution Vulnerability

- Add

- Add Bookmark or Share

- Google+
- Technorati
- Digg
- Delicious
- Reddit
- StumbleUpon
- Twitter
- LinkedIn
- Facebook
- Newsvine

Microsoft Windows Media Center CVE-2015-2509 Remote Code Execution Vulnerability

Risk

High

Date Discovered

September 8, 2015

Description

Microsoft Windows Media Center is prone to a remote code-execution vulnerability. An attacker can leverage this issue to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial-of-service conditions.

Technologies Affected

- Microsoft Windows 7 for 32-bit Systems SP1
- Microsoft Windows 7 for x64-based Systems SP1
- Microsoft Windows 8 for 32-bit Systems
- Microsoft Windows 8 for x64-based Systems
- Microsoft Windows 8.1 for 32-bit Systems
- Microsoft Windows 8.1 for x64-based Systems
- Microsoft Windows Media Center
- Microsoft Windows Vista Service Pack 2
- Microsoft Windows Vista x64 Edition Service Pack 2

Recommendations

Run all software as a nonprivileged user with minimal access rights.

To reduce the impact of latent vulnerabilities, always run nonadministrative software as an unprivileged user with minimal access rights.

Deploy network intrusion detection systems to monitor network traffic for malicious activity.

Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity. This includes but is not limited to requests that include NOP sleds and unexplained incoming and outgoing traffic. This may indicate exploit attempts or activity that results from a successful exploit.

Do not accept or execute files from untrusted or unknown sources.

To reduce the likelihood of successful attacks, never handle or open files from unknown sources.

Do not follow links provided by unknown or untrusted sources.

To reduce the likelihood of successful exploits, never visit sites of questionable integrity or follow links provided by unfamiliar or untrusted sources.

Implement multiple redundant layers of security.

As this issue may be cause by a memory-corruption error, consider various memory-protection schemes (such as nonexecutable and randomly mapped memory segments) that may hinder an attacker's ability to exploit memory-corruption vulnerabilities. Host-based intrusion-prevention systems may also help prevent exploits.
Updates are available. Please see the references or vendor advisory for more information.

References

- Microsoft - Microsoft Homepage

Credits

Aaron Luo, Kenney Lu, and Ziv Chang of TrendMicro

Disclaimer
The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.
Symantec, Symantec products, Symantec Security Response, and secure@symantec.com are registered trademarks of Symantec Corp. and/or

Threat Intelligence

Security Response 10h
@threatintel

You can find Symantec's blog post on MSFT's September #PatchTuesday updates here: symc.ly/1ib5khQ pic.twitter.com/d14yJQ9W67

Show Photo

Security Response 15h
@threatintel

Robot left incapacitated after brutal attack, investigators say he's now slower and may have damaged internal systems japantimes.co.jp/news/2015/09/0

Show Summary

Security Response 18h
@threatintel

Alleged key players behind #BankingMalware Dridex and Citadel arrested by European police krebsonsecurity.com/2015/09/ar

Expand

Follow the Threat Intelligence Twitter feed

STAR Malware Protection Technologies
The security technologies Symantec creates
Learn more

- About Symantec|
- Careers|
- Events|
- News|
- Site Map|
- Legal|
  - Legal Notices
  - License Agreements
  - Repository
  - Customer Trust Portal
- Privacy|
- Cookies|
- Contact|
  - Norton Support
  - Business Support
  - Business Sales
  - Customer Support
  - Authentication Services
  - Corporate Information
- RSS