Microsoft Security Advisory 2269637

By BetaFred

Insecure Library Loading Could Allow Remote Code Execution

Published: August 23, 2010 | Updated: May 13, 2014

Version: 19.0

General Information

Executive Summary

Microsoft is aware that research has been published detailing a remote attack vector for a class of vulnerabilities that affects how applications load external libraries.

This issue is caused by specific insecure programming practices that allow so-called "binary planting" or "DLL preloading attacks". These practices could allow an attacker to remotely execute arbitrary code in the context of the user running the vulnerable application when the user opens a file from an untrusted location.

This issue is caused by applications passing an insufficiently qualified path when loading an external library. Microsoft has issued guidance to developers in the MSDN article, Dynamic-Link Library Security, on how to correctly use the available application programming interfaces to prevent this class of vulnerability. Microsoft is also actively reaching out to third-party vendors through the Microsoft Vulnerability Research Program to inform them of the mitigations available in the operating system. Microsoft is also actively investigating which of its own applications may be affected.

In addition to this guidance, Microsoft is releasing a tool that allows system administrators to mitigate the risk of this new attack vector by altering the library loading behavior system-wide or for specific applications. This advisory describes the functionality of this tool and other actions that customers can take to help protect their systems.

Mitigating Factors:

- This issue only affects applications that do not load external libraries securely. Microsoft has previously published guidelines for developers in the MSDN article, Dynamic-Link Library Security, that recommend alternate methods to load libraries that are safe against these attacks.
- For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a document from this location that is then loaded by a vulnerable application.
- The file sharing protocol SMB is often disabled on the perimeter firewall. This limits the possible attack vectors for this vulnerability.

Updates relating to Insecure Library Loading:

Update released on November 9, 2010

- Microsoft Security Bulletin MS10-087, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on December 14, 2010

- Microsoft Security Bulletin MS10-093, "Vulnerability in Windows Movie Maker Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS10-094, "Vulnerability in Windows Media Encoder Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS10-095, "Vulnerability in Microsoft Windows Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS10-096, "Vulnerability in Windows Address Book Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS10-097, "Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on January 11, 2011

- Microsoft Security Bulletin MS11-001, "Vulnerability in Windows Backup Manager Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on February 8, 2011

- Microsoft Security Bulletin MS11-003, "Cumulative Security Update for Internet Explorer," provides support for a vulnerable component of Internet Explorer that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on March 8, 2011

- Microsoft Security Bulletin MS11-015, "Vulnerabilities in Windows Media Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS11-016, "Vulnerability in Microsoft Groove Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

- Microsoft Security Bulletin MS11-017, "Vulnerability in Remote Desktop Client Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on April 12, 2011

- Microsoft Security Bulletin MS11-023, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS11-025, "Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution," provides support for a vulnerable component in certain applications built using the Microsoft Foundation Class (MFC) Library that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on July 12, 2011

- The update in Microsoft Knowledge Base Article 2533623 implements Application Programming Interface (API) enhancements in Windows to help developers correctly and securely load external libraries. This update for Windows is available in the "High Priority" Updates category for customers who have not already received the update through automatic updating.

  Developers can help to ensure their programs load DLLs properly to avoid "DLL preloading" or "binary planting" attacks by following the guidance provided in Microsoft Knowledge Base Article 2533623 to take advantage of the API enhancements provided by this update.

- Microsoft Security Bulletin MS11-055, "Vulnerability in Microsoft Visio Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on August 9, 2011

- Microsoft Security Bulletin MS11-059, "Vulnerability in Data Access Components Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on September 13, 2011

- Microsoft Security Bulletin MS11-071, "Vulnerability in Windows Components Could Allow Remote Code Execution," provides support for vulnerable components of Microsoft Windows that are affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS11-073, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution," provides support for vulnerable components of Microsoft Office that are affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on October 11, 2011

- Microsoft Security Bulletin MS11-075, "Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS11-076, "Vulnerability in Windows Media Center Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on November 8, 2011

- Microsoft Security Bulletin MS11-085, "Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on December 13, 2011

- Microsoft Security Bulletin MS11-099, "Cumulative Security Update for Internet Explorer," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS11-094, "Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Updates released on February 14, 2012

- Microsoft Security Bulletin MS12-012, "Vulnerability in Color Control Panel Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.
- Microsoft Security Bulletin MS12-014, "Vulnerability in Indeo Codec Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Windows that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on March 13, 2012

- Microsoft Security Bulletin MS12-022, "Vulnerability in Expression Design Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Expression Design that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on June 12, 2012

- Microsoft Security Bulletin MS12-039, "Vulnerabilities in Lync Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Lync that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on July 10, 2012

- Microsoft Security Bulletin MS12-046, "Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Visual Basic for

Applications that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on November 13, 2012

- Microsoft Security Bulletin MS12-074, "Vulnerabilities in .NET Framework Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft .NET Framework that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Update released on May 13, 2014

- Microsoft Security Bulletin MS14-023, "Vulnerability in Microsoft Office Could Allow Remote Code Execution," provides support for a vulnerable component of Microsoft Office that is affected by the Insecure Library Loading class of vulnerabilities described in this advisory.

Affected Software

Microsoft is investigating whether any of its own applications are affected by insecure library loading vulnerabilities and will take appropriate action to protect its customers.

Advisory FAQ

Where can developers find guidance on how to avoid this issue?
As of June 14, 2011, the update in Microsoft Knowledge Base Article 2533623 implements Application Programming Interface (API) enhancements in Windows to help developers correctly and securely load external libraries. Developers should follow the guidance provided in Microsoft Knowledge Base Article 2533623 to take advantage of the API enhancements provided by the update.

Microsoft has also published the MSDN article, Dynamic-Link Library Security, which describes the various Application Programming Interfaces (APIs) available on Windows that allow developers to correctly and securely load external libraries.

Microsoft is working with developers through the Microsoft Vulnerability Research Program to share information with them on how to prevent this vulnerability in their products. Software vendors and ISVs that have questions on the mitigations available in Windows for this issue are invited to contact for additional mitigation information.

What is the scope of the issue?
Microsoft is aware of research published by a number of security researchers that describes a new remote attack vector for this known class of vulnerabilities. Applications are affected when they insufficiently qualify the path of an external library.

What causes this threat?
This exploit may occur when applications do not directly specify the fully qualified path to a library it intends to load. Depending on how the application is developed, Windows, instructed by the application, will search specific locations in the file system for the necessary library, and will load the file if found.

Some Application Programming Interfaces (API), such as SearchPath, use a search order that is intended for documents and not application libraries. Applications that use this API may try to load the library from the Current Working Directory (CWD), which may be controlled by an attacker. Other APIs may also lead to similar behavior, when used in specific ways described in the MSDN article, Dynamic-Link Library Security.

In the case of network shares, such as WebDAV or SMB, an attacker who can write to this location could upload a specially crafted library. In this scenario, the application attempts to load the specially crafted library, which can then execute arbitrary code on the client system in the security context of the logged-on user.

What might an attacker use this vulnerability to do?
An attacker who successfully exploited this vulnerability could gain the same user rights as a logged-on user. If the user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

In some cases, an attacker who already has access to a local folder on the system could use a DLL preloading vulnerability in a local application running with elevated privileges to elevate his access to the system.

How could an attacker exploit this vulnerability?
This vulnerability requires that the attacker convince the user to open a file using a vulnerable program, from a remote network location. When the application loads one of its required or optional libraries, the vulnerable application may attempt to load the library from the remote network location. If the attacker provides a specially crafted library at this location, the attacker may succeed at executing arbitrary code on the user's machine.

What are the remote attack vectors for this vulnerability?
This vulnerability can be exploited over network file systems such as (but not limited to) WebDAV and SMB. An attacker can offer a file for download over any such protocol. If the application used to open this file does not load external libraries securely, the user opening that file could be exposed to this vulnerability.

Is this a security vulnerability that requires Microsoft to issue a security update?
This vulnerability may require third-party vendors to issue a security update for their respective affected applications. As part of this security advisory, Microsoft is releasing an optional mitigation tool that helps customers address the risk of the remote attack vector through a per-application and global configuration setting.

Microsoft is also investigating whether any of its own applications are affected by DLL preloading vulnerabilities and will take appropriate action to protect its customers.

What is a Dynamic Link Library (DLL)?
A DLL is a library that contains code and data that can be used by more than one program at the same time. For example, in Windows operating systems, the Comdlg32 DLL performs common dialog box related functions. Therefore, each program can use the functionality that is contained in this DLL to implement an Open dialog box. This helps promote code reuse and efficient memory usage.

By using a DLL, a program can be modularized into separate components. For example, an accounting program may be sold by module. Each module can be loaded into the main program at run time if that module is installed.

Because the modules are separate, the load time of the program is faster, and a module is only loaded when that functionality is requested.

What is Web-based Distributed Authoring and Versioning (WebDAV)?
Web-based Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web. Integrated into IIS, WebDAV allows clients to do the following:

- Manipulate resources in a WebDAV publishing directory on your server. For example, users who have been assigned the correct rights can copy and move files around in a WebDAV directory.
- Modify properties associated with certain resources. For example, a user can write to and retrieve a file's property information.
- Lock and unlock resources so that multiple users can read a file concurrently.
- Search the content and properties of files in a WebDAV directory.

What is Microsoft Server Message Block (SMB) protocol?
Microsoft Server Message Block (SMB) Protocol is a Microsoft network file sharing protocol used in Microsoft Windows. For more information on SMB, see MSDN article, Microsoft SMB Protocol and CIFS Protocol Overview.

Suggested Actions

- **Apply the update for affected software**

  Refer to the section, **Updates relating to Insecure Library Loading**, for available updates.

- **Apply Workarounds**

  Workarounds refer to a setting or configuration change that does not correct the underlying issue but would help block known attack vectors before a security update is available. See the next section, **Workarounds**, for more information.

Workarounds

- **Disable loading of libraries from WebDAV and remote network shares**

  Note See Microsoft Knowledge Base Article 2264107 to deploy a workaround tool that allows customers to disable the loading of libraries from remote network or WebDAV shares. This tool can be configured to disallow insecure loading on a per-application or a global system basis.

  Customers who are informed by their vendor of an application being vulnerable can use this tool to help protect against attempts to exploit this issue.

  Note See Microsoft Knowledge Base Article 2264107 to use the automated **Microsoft Fix it** solution to deploy the registry key to block loading of libraries for SMB and WebDAV shares. Note that this Fix it solution does require you to install the workaround tool also described in Microsoft Knowledge Base Article 2264107 first. This Fix it solution only deploys the registry key and requires the workaround tool in

order to be effective. We recommend that administrators review the KB article closely prior to deploying this Fix it solution.

** **

- **Disable the WebClient service**

  Disabling the WebClient service helps protect affected systems from attempts to exploit this vulnerability by blocking the most likely remote attack vector through the Web Distributed Authoring and Versioning (WebDAV) client service. After applying this workaround it is still possible for remote attackers who successfully exploit this vulnerability to cause the system to run programs located on the targeted user's computer or the Local Area Network (LAN), but users will be prompted for confirmation before opening arbitrary programs from the Internet.

  To disable the WebClient Service, follow these steps:

  1. Click **Start**, click **Run**, type **Services.msc** and then click **OK**.
  2. Right-click **WebClient** service and select **Properties**.
  3. Change the Startup type to **Disabled**. If the service is running, click **Stop**.
  4. Click **OK** and exit the management application.

  Impact of workaround. When the WebClient service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted. In addition, any services that explicitly depend on the Web Client service will not start, and an error message will be logged in the System log. For example, WebDAV shares will be inaccessible from the client computer.

  How to undo the workaround.

  To re-enable the WebClient Service, follow these steps:

  1. Click **Start**, click **Run**, type **Services.msc** and then click **OK**.
  2. Right-click **WebClient** service and select **Properties**.
  3. Change the Startup type to **Automatic**. If the service is not running, click **Start**.
  4. Click **OK** and exit the management application.

- **Block TCP ports 139 and 445 at the firewall**

  These ports are used to initiate a connection with the affected component. Blocking TCP ports 139 and 445 at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. Microsoft recommends that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, see the TechNet article, TCP and UDP Port Assignments.

  Impact of workaround. Several Windows services use the affected ports. Blocking connectivity to the ports may cause various applications or services to not function. Some of the applications or services that could be impacted are listed below:

- Applications that use SMB (CIFS)
- Applications that use mailslots or named pipes (RPC over SMB)
- Server (File and Print Sharing)
- Group Policy
- Net Logon
- Distributed File System (DFS)
- Terminal Server Licensing
- Print Spooler
- Computer Browser
- Remote Procedure Call Locator
- Fax Service
- Indexing Service
- Performance Logs and Alerts
- Systems Management Server
- License Logging Service

How to undo the workaround. Unblock TCP ports 139 and 445 at the firewall. For more information about ports, see TCP and UDP Port Assignments.

Additional Suggested Actions

- **Install updates from third-party vendors that address insecure library loading**

  Third-party vendors may release updates that address insecure library loading in their products. Microsoft recommends that customers contact their vendor if they have any questions whether or not a specific application is affected by this issue, and monitor for security updates released by these vendors.

- **Protect your PC**

  We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates and installing antivirus software. For more information, see Microsoft Safety & Security Center.

- **Keep Microsoft Software Updated**

  Users running Microsoft software should apply the latest Microsoft security updates to help make sure that their computers are as protected as possible. If you are not sure whether your software is up to date, visit Microsoft Update, scan your computer for available updates, and install any high-priority updates that are offered to you. If you have automatic updating enabled and configured to provide updates for Microsoft products, the updates are delivered to you when they are released, but you should verify that they are installed.

Other Information

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners.

Feedback

- You can provide feedback by completing the Microsoft Help and Support form, Customer Service Contact Us.

Support

- Customers in the United States and Canada can receive technical support from Security Support. For more information, see Microsoft Help and Support.
- International customers can receive support from their local Microsoft subsidiaries. For more information, see International Support.
- Microsoft TechNet Security provides additional information about security in Microsoft products.

Disclaimer

The information provided in this advisory is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (August 23, 2010): Advisory published.
- V1.1 (August 31, 2010): Added a link to Microsoft Knowledge Base Article 2264107 to provide an automated **Microsoft Fix it** solution for the workaround, Disable loading of libraries from WebDAV and remote network shares.
- V2.0 (November 9, 2010): Added Microsoft Security Bulletin MS10-087, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution," to the **Updates relating to Insecure Library Loading** section.
- V3.0 (December 14, 2010): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS10-093, "Vulnerability in Windows Movie Maker Could Allow Remote Code Execution;" MS10-094, "Vulnerability in Windows Media Encoder Could Allow Remote Code Execution;" MS10-095, "Vulnerability in Microsoft Windows Could Allow Remote Code

Execution;" MS10-096, "Vulnerability in Windows Address Book Could Allow Remote Code Execution;" and MS10-097, "Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution."

- V4.0 (January 11, 2011): Added Microsoft Security Bulletin MS11-001, "Vulnerability in Windows Backup Manager Could Allow Remote Code Execution," to the **Updates relating to Insecure Library Loading** section.
- V5.0 (February 8, 2011): Added Microsoft Security Bulletin MS11-003, "Cumulative Security Update for Internet Explorer," to the **Updates relating to Insecure Library Loading** section.
- V6.0 (March 8, 2011): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS11-015, "Vulnerabilities in Windows Media Could Allow Remote Code Execution;" MS11-016, "Vulnerability in Microsoft Groove Could Allow Remote Code Execution;" and MS11-017, "Vulnerability in Remote Desktop Client Could Allow Remote Code Execution."
- V7.0 (April 12, 2011): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS11-023, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution;" and MS11-025, "Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution."
- V8.0 (July 12, 2011): Added the update in Microsoft Knowledge Base Article 2533623 and the update in Microsoft Security Bulletin MS11-055, "Vulnerability in Microsoft Visio Could Allow Remote Code Execution," to the **Updates relating to Insecure Library Loading** section. The update in Microsoft Knowledge Base Article 2533623 implements Application Programming Interface (API) enhancements in Windows to help developers correctly and securely load external libraries.
- V9.0 (August 9, 2011): Added Microsoft Security Bulletin MS11-059, "Vulnerability in Data Access Components Could Allow Remote Code Execution," to the **Updates relating to Insecure Library Loading** section.
- V10.0 (September 13, 2011): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS11-071, "Vulnerability in Windows Components Could Allow Remote Code Execution;" and MS11-073, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution."
- V11.0 (October 11, 2011): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS11-075, "Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution;" and MS11-076, "Vulnerability in Windows Media Center Could Allow Remote Code Execution."
- V12.0 (November 8, 2011): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS11-085, "Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution."
- V13.0 (December 13, 2011): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS11-099, "Cumulative Security Update for Internet Explorer;" and MS11-094, "Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution."
- V14.0 (February 14, 2012): Added the following Microsoft Security Bulletins to the **Updates relating to Insecure Library Loading** section: MS12-012, "Vulnerability in Color Control Panel Could Allow Remote Code Execution;" and MS12-014, "Vulnerability in Indeo Codec Could Allow Remote Code Execution."

- V15.0 (March 13, 2012): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS12-022, "Vulnerability in Expression Design Could Allow Remote Code Execution."
- V16.0 (June 12, 2012): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS12-039, "Vulnerabilities in Lync Could Allow Remote Code Execution."
- V17.0 (July 10, 2012): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS12-046, "Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution."
- V18.0 (November 13, 2012): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS12-074, "Vulnerabilities in .NET Framework Could Allow Remote Code Execution."
- V19.0 (May 13, 2014): Added the following Microsoft Security Bulletin to the **Updates relating to Insecure Library Loading** section: MS14-023, "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution."

Page generated 2014-05-12 18:40Z-07:00.
