

Cisco Customer Contact Software Policy for using Microsoft security updates on products deployed on a retail installation of Windows operating system

PB455396

Scope

This product bulletin outlines the Cisco® policy and guidelines for installing security updates that Microsoft issues for the Windows Operating System, Internet Information Server (IIS), and Sequenced Query Language (SQL) Server on Cisco Unified Customer Contact products that are deployed on standard retail packaged installations of the Windows Operating System. The following Cisco Customer Contact software products fall into this category:

- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Intelligent Contact Management Hosted
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Hosted
- Cisco Unified Customer Voice Portal

Policy and Guidelines

The Cisco Unified Customer Contact software products listed previously require customers to license and install the Windows Operating System, Microsoft IIS, and SQL Server. Microsoft issues security updates on the second Tuesday of each month. Because customers license these products from third parties and not from Cisco, customers are responsible for monitoring the availability of these security updates.

Cisco qualifies the previously listed customer contact software products with the latest Microsoft security update for the last two supported versions of the software and only on the supported version of the Windows Operating System. Cisco issues an Impact Assessment bulletin, typically a few days after the second Tuesday of the month, which categorizes the effect of Microsoft security updates on these customer contact software products. Cisco recommends that customers assess the security exposure of the critical security patches released by Microsoft for Windows, IIS and SQL and apply critical security patches as deemed necessary for their site ahead of Cisco's Impact Assessment bulletin.

For older versions of the Cisco Unified Customer Contact software products, Cisco recommends that customers review any security update issued for these products and assess their exposure to the vulnerability. If deemed necessary, customers should follow Microsoft's guidelines to apply these updates to the relevant systems as soon as possible. Cisco qualifies older versions of Cisco Unified Customer Contact software products on an as-needed basis.

Cisco categorizes the effect that every Microsoft security update has on the previously listed Cisco Unified Customer Contact software products based on the following Cisco defined categories:

- **Impacting:** Microsoft labels the update as critical, important, or otherwise of special interest, and it directly affect the Cisco Unified Customer Contact software product. In other words, the update affects some software component or function (or is basic to the operating system and affects all operations for any software), or it applies to the latest supported Cisco Unified Customer Contact software product qualified service pack(s). Cisco recommends installing such an update. In the unlikely event that problems are found with a particular update, Cisco tests and qualifies the faults before approving the use of the security update with Cisco Unified Customer Contact software products.
- **Deferred:** Microsoft labels the update as critical, important, or is otherwise of special interest, but it does not directly affect Cisco Unified Customer Contact software product components or functions during regular use of the software. Qualification testing is typically deferred and performed with the next maintenance release of the product. The release notes of the maintenance release describe the applicability of all security updates relative to that maintenance release.
- **Not applicable:** The update does not apply to the latest supported Cisco Unified Customer Contact software product, regardless of product applicability or Microsoft rated severity. Cisco performs no additional qualification testing.

Impact Assessment Bulletin

Until April 2008, all Microsoft security update assessment notices were published as Field Notices. Starting May 2008, the Impact Assessment bulletin is published on Cisco Security Center and is available as a free RSS feed. You can obtain the Impact Assessment bulletin by visiting Cisco Security Center at <http://www.cisco.com/security>, click on IntelliShield Event Responses, select the month/year of the bulletin required, and then look for **Cisco Contact Center and Self Service Products Impact Assessment** section. You can also subscribe to the IntelliShield Event Responses RSS feed at http://tools.cisco.com/security/center/eventResponses_20.xml.

Important Note

This policy applies only to Microsoft security updates. It does not apply to Microsoft service packs. Microsoft service packs contain a broad range of fixes and updates, and Cisco needs to verify them before they can be applied. For every release, Cisco explicitly specifies the Microsoft service packs that are required and supported.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)