

Cisco Security Advisory: Cisco Secure Desktop ActiveX Control Code Execution Vulnerability

Advisory ID: [cisco-sa-20100414-csd](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20100414-csd.shtml>

Revision 1.1

Last Updated 2010 July 13 1400 UTC (GMT)

For Public Release 2010 April 14 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Cisco Secure Desktop contains a vulnerable ActiveX control that could allow an attacker to execute arbitrary code with the privileges of the user who is currently logged into the affected system. Cisco has released a free software update that addresses this vulnerability. There is a workaround that mitigates this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100414-csd.shtml>.

[\[Expand all sections\]](#) | [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

Cisco Secure Desktop versions prior to 3.5.841 are affected.

☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

A Cisco-signed ActiveX control that is used by Cisco Secure Desktop fails to properly verify the integrity of an executable file that is used by the Cisco Secure Desktop installation process. If an attacker can entice a user to visit an attacker controlled web page, the vulnerable ActiveX control could be invoked to download an attacker-modified package. The package could contain a malicious executable file that executes with the privileges of the affected user. A successful exploit could result in a complete compromise of a vulnerable system. This vulnerability is documented in Cisco Bug ID [CSCta25876](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2010-0589.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

[CSCta25876](#) ([registered](#) customers only)

Calculate the environmental score of [CSCta25876](#)

CVSS Base Score - **9.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - 7.7					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

Impact

Successful exploitation of this vulnerability could result in a complete compromise of the affected system.

[Top of the section](#) [Close Section](#)

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco Secure Desktop version 3.5.841 can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=3.5.841&mdfid=280277835&sftType=CSD+package+ASA+Distribution&optPlat=&nodecount=2&edesignator=null&modelName=Cisco+Secure+Desktop&treeMdfid=268438162&treeName=Security&modifmdfid=null&imname=&hybrid=&imst=&lr=Y>

Note: Cisco Secure Desktop versions 3.0 and 3.1 are only supported for operation with certain versions of Cisco IOS software and Cisco Adaptive Security Appliance (ASA) software version 7.x. Cisco Secure Desktop versions 3.2 through 3.5 are only supported for operation with Cisco ASA software version 8.x. Customers running Cisco Secure Desktop versions 3.2 through 3.5 with a supported Cisco ASA software version are encouraged to upgrade to Cisco Secure Desktop version 3.5.841.

Customers with active software licenses for Cisco Secure Desktop versions 3.0 and 3.1 should send email to the following address for instructions on migrating to non-vulnerable software:

csd-activex-inquiry@cisco.com

[Top of the section](#) [Close Section](#)

Workarounds

Administrators can mitigate this vulnerability by using the kill bit feature of Microsoft Windows to prevent the loading and execution of the vulnerable ActiveX control. Administrators must use the Class identifier (CLSID) of the vulnerable ActiveX control to disable the control. The affected CLSID is:

705EC6D4-B138-4079-A307-EF13E4889A82

Instructions for setting the kill bit in Microsoft Windows are available at the following link:

<http://support.microsoft.com/kb/240797>

Note: Kill bit settings are permanent. The settings must be removed to regain Cisco Secure Desktop functionality. After an administrator has updated the Cisco Secure Desktop software to a fixed version on VPN portal devices, the kill bit must be removed from Microsoft Windows clients in order to allow the Cisco Secure Desktop software to be upgraded. Once the kill bit is removed, clients may be vulnerable until a fixed Cisco Secure Desktop version is installed.

Update: Cisco Secure Desktop software version 3.5.1077 replaces the old, vulnerable ActiveX CLSID with a newly issued CLSID. New installations and upgrading from an older version of Cisco Secure Desktop will use the new CLSID. Once the software upgrade has been installed on client systems, administrators can safely and permanently implement the ActiveX kill bit workaround for the old CLSID in their environment.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20100414-csd.shtml>

[Top of the section](#) [Close Section](#)

Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.htm, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact psirt@cisco.com or security-alert@cisco.com for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-

party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was discovered and reported to Cisco by an anonymous researcher working with TippingPoint's Zero Day Initiative. Cisco would like to thank TippingPoint for reporting this vulnerability and collaborating on a coordinated disclosure.

[Top of the section](#) [Close Section](#)

☐ Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

▣ Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20100414-csd.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

▣ Revision History

Revision 1.1	2010-July-13	Updated workarounds.
Revision 1.0	2010-April-14	Initial public release.

[Top of the section](#) [Close Section](#)

▣ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#) [Close Section](#)

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)