

Cisco Collaboration Server 5.0: Troubleshooting Security Vulnerability Caused by the HTTP TRACE/TRACK Methods

Document ID: 107523

Introduction

Prerequisites

Requirements

Components Used

Conventions

Webserver HTTP TRACE/TRACK Method Support Cross-Site Tracing Vulnerability Install and Configure URLScan Utility Version 2.5 to Disable HTTP TRACE/TRACK Method

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document addresses the steps to work around the security vulnerability caused by the HTTP TRACE/TRACK methods for products that use Microsoft Internet Information Services (IIS) as the webserver. Cisco Collaboration Server 5.0 uses IIS 5.0 as the webserver and is susceptible to this vulnerability. The solution is to use Microsoft's URLScan utility to disable the HTTP TRACE/TRACK methods.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Microsoft Windows 2000 Server
- Cisco Collaboration Server 5.0
- Microsoft IIS 5.0
- Microsoft URLScan utility

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 2000
- Cisco Collaboration Server versions 5.0
- Microsoft IIS 5 (when using Windows 2000)
- Microsoft URLScan 2.5

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Webserver HTTP TRACE/TRACK Method Support

Cross-Site Tracing Vulnerability

A webserver was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the webserver. Per the HTTP specification, when this method is used, the webserver echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS Webserver uses an alias TRACK for this method, and is functionally the same.

A vulnerability related to this method was discovered. A malicious, active component in a web page can send TRACE requests to a webserver that supports this TRACE method. Usually, browser security disallows access to websites outside of the present site's domain. Although unlikely and difficult to achieve, it is possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary websevers beyond the hosting webserver. Because the chosen webserver then echoes back the client request unfiltered, the response also includes cookie-based or web-based (if logged on) authentication credentials that the browser automatically sent to the specified web application on the specified webserver. The significance of the TRACE capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but receives it after the target webserver echoes it back as TRACE response. Because this vulnerability exists as a support for a method required by the HTTP protocol specification, most common websevers are vulnerable.

Microsoft IIS: Microsoft released URLScan

(<http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp>), which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases TRACK to TRACE. Therefore, if URLScan is used to specifically block the TRACE method, the TRACK method should also be added to the filter. URLScan uses the urlscan.ini configuration file, usually in `\System32\InetSrv\URLScan` directory.

In that, there are two sections: `AllowVerbs` and `DenyVerbs`. The former is used if the `UseAllowVerbs` variable is set to **1**; otherwise (if set to 0), the `DenyVerbs` are used. Clearly, either can be used, depending on whether you want a `Default-Deny-Explicit-Allow` or a `Default-Allow-Explicit-Deny` policy. In order to disallow TRACE and TRACK methods through URLScan, first remove TRACK, TRACE methods from the `AllowVerbs` section and add them to the `DenyVerbs` section. With this, URLScan will disallow all TRACE and TRACK methods, and generate an error page for all requests using that method. In order to enable the changes, restart the World Wide Web Publishing Service from the **Services > Control Panel** item.

Install and Configure URLScan Utility Version 2.5 to Disable HTTP TRACE/TRACK Method

Complete these steps:

1. Install URLScan 2.5 in the Cisco Collaboration Server. In order to download URLScan 2.5, refer to this Microsoft website:

<http://microsoft.com/downloads/details.aspx?FamilyId=23D18937-DD7E-4613-9928-7F94EF1C902A&dis>

2. Edit the urlscan.ini property file present in **<Windows 2000 Server install drive>:\WINNT\system32\inetsrv\urlscan**.
3. Change the `AllowDotInPath` property from 0 to 1. By default, URLScan does not allow dots in URLs, and the Cisco Collaboration Server requires this property to be set to 1 (agents will not be able to login if this property is set to 0).
4. Add the TRACE and TRACK methods under the `DenyVerbs` section, and change the `AllowVerbs` property from 1 to 0.

5. Restart Internet Information Services(IIS)/World Wide Web services from the **Services > Control Panel** item on the Cisco Collaboration Server.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Customer Contact Software

IP Communications and Video: Contact Center

Related Information

- **Technical Support & Documentation – Cisco Systems**
-

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

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 02, 2008

Document ID: 107523
