

Securiteam: [NEWS] TCLHttpd Contains Two Vulnerabilities (Directory Browsing, XSS)

[NEWS] TCLHttpd Contains Two Vulnerabilities (Directory Browsing, XSS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/01/03

To: list@securiteam.com

Date: 1 Oct 2003 11:49:29 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

TCLHttpd Contains Two Vulnerabilities (Directory Browsing, XSS)

SUMMARY

<<http://www.tcl.tk/software/tclhttpd>> TCLHttpd is "used both as a general-purpose Web server, and as a framework for building server applications. It implements Tcl (<http://www.tcl.tk>), including the Tcl Resource Center and Scriptics' electronic commerce facilities. It is also built into several commercial applications such as license servers and mail spam filters. Instructions for setting up the TclHttpd on your platform are given towards the end of the chapter, on page see the TclHttpd Distribution. It works on UNIX, Windows, and Macintosh. You can have the server up and running quickly".

The product has been found to contain two security vulnerabilities that would allow a remote attacker to view the directory and file contents of directories residing on the server, and to cause the product to return arbitrary content as if it were its own.

DETAILS

Vulnerable systems:

* TCLHttpd version 3.4.2

Securiteam: [NEWS] TCLHttpd Contains Two Vulnerabilities (Directory Browsing, XSS)

Multiple flaws in TCLHttpd server which open door for an attacker to browse any directories on the remote host, and to inject malicious JavaScript/VBScript content to the user's browser under the TCLHttpd server context (Cross Site Scripting).

Arbitrary Directory Browsing

When a user requests a directory on TCLHttpd server, httpdthread.tcl will start to look for various default index file names in that directory, if none can be found then it will pass the operation to dirlist.tcl script to do the "fancy" directory listing which provides users the ability to sort files by modify date, name, size or file's pattern. Dirlist.tcl script does filter inputs from the users in order to prevent directory traversal but it can be easily bypassed if an absolute path was entered. Directory listing is enabled by default.

For example:

Requesting http://abc.com/images/?pattern=/*&sort=name will return you a list of directory under /

Cross Site Scripting (XSS)

TCLHttpd web server comes with various modules in order to increase the flexibility of the server, and /debug module is enable by default which allows you to download logging information, debug the Tcl part of the application without restarting the hosting application. Many modules are suffered from the multiple Cross Site Scripting (XSS) vulnerabilities that potentially enable a malicious user to "inject" code into a user's session under TCLHttpd server context. Phuong is going to use the /debug module as an example.

[http://www.abc.com/debug/echo?name=>alert\('hello'\);</script>](http://www.abc.com/debug/echo?name=>alert('hello');</script>)
[http://www.abc.com/debug/dbg?host=>alert\('hello'\);</script>](http://www.abc.com/debug/dbg?host=>alert('hello');</script>)
[http://www.abc.com/debug/showproc?proc=>alert\('hello'\);</script>](http://www.abc.com/debug/showproc?proc=>alert('hello');</script>)
[http://www.abc.com/debug/errorInfo?title=>alert\('hello'\);</script>](http://www.abc.com/debug/errorInfo?title=>alert('hello');</script>)

Workaround:

You can eliminate the threats from these vulnerabilities by editing your httpdthread.tcl and comment out the directory listing option, also you should disable the following modules to prevent Cross Site Scripting: Status, Debug, Mail, and Admin.

Notes: Disabling some modules in your TCLHttpd configuration might decrease the flexibility of your server.

Vendor status:

Vendor has been notified.

ADDITIONAL INFORMATION

The information has been provided by <mailto:dphuong@yahoo.com> Phuong Nguyen.

Securiteam: [NEWS] TCLHttpd Contains Two Vulnerabilities (Directory Browsing, XSS)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.