

[NT] Xedus Webserver Directory Traversal and DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0008.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/02/04

To: list@securiteam.com

Date: 2 Sep 2004 14:08:23 +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>

Xedus Webserver Directory Traversal and DoS

SUMMARY

<<http://www.thinxoft.com>> Xedus is a Peer-to-Peer web server and provides you with the ability to share files, music, and any other media, as well as create robust and dynamic web sites, which can feature database access, file system access, with full .net support.

The Xedus web server is vulnerable to a directory traversal. In addition some test scripts provided with the default installation are prone to cross-site scripting (XSS). The server is also vulnerable to a DoS condition.

DETAILS

Vulnerable Systems:

* Xedus web server version 1.0

Xedus web server cannot handle multiple connections from the same host, and will deny all access to any users after a number of connections are made from a malicious user. This vulnerability can be leveraged by an attacker to deny all requests to a website, thus rendering it

Securiteam: [NT] Xedus Webserver Directory Traversal and DoS

inaccessible. Although simple, this vulnerability constitutes a denial of service vulnerability.

Xedus is also vulnerable to directory traversal that allows an attacker to reach parts of the file system that are normally not even served by the web server. Served files are files residing in the docs directory (Apache's htdocs for example) and in any other directory that the server is configured to serve from. The web server does not properly sanitize requests received by clients. This vulnerability can be exploited to retrieve arbitrary, potentially sensitive files from the hosting computer with the privileges of the web server. This may aid a malicious user in further attacks. Typical examples are:

<http://host:4274/./data/log.txt>

<http://host:4274/./././././././boot.ini>

<http://host:4274/././././././WINNT/repair/sam>

It should be noted, that by default the Xedus web server listens for incoming connections on port 4274, however this value can be edited by the administrator of the Xedus web server.

The last vulnerability is not a vulnerability of the server software itself but of the test scripts that are provided with it in a default installation. The scripts are prone to XSS attacks, examples following:

[http://host:4274/test.x?username=\[XSS\]](http://host:4274/test.x?username=[XSS])

[http://host:4274/TestServer.x?username=\[XSS\]](http://host:4274/TestServer.x?username=[XSS])

[http://host:4274/testgetrequest.x?param=\[XSS\]](http://host:4274/testgetrequest.x?param=[XSS])

The input received by some of these test scripts is not properly sanitized. Because the input is not properly sanitized, it allows for an attacker to send a malicious URL that will then render malicious code in the context of a victim's web browser.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@gulftech.org> GulfTech Security.

The original article can be found at:

<http://www.gulftech.org/?node=research&article_id=00047-08302004>

http://www.gulftech.org/?node=research&article_id=00047-08302004

=====

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

=====

=====

Securiteam: [NT] Xedus Webserver Directory Traversal and DoS

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.