

[NT] SurgeLDAP Multiple Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0035.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/13/03

To: list@securiteam.com

Date: 13 Aug 2003 14:31:29 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

SurgeLDAP Multiple Security Vulnerabilities

SUMMARY

<<http://netwinsite.com/surgeldap/>> SurgeLDAP is "an advanced easy to manage and install high performance LDAP v3 server. It supports any number of schemas, easy to add/modify existing schemas, integrated web based user access, and fast browser based administration tools. And all relevant RFC protocols LDAP v2, LDAP v3, HTTP". The product has been found to contain multiple security vulnerabilities.

DETAILS

The following vulnerabilities have been found in the SurgeLDAP product:

- 1) Disclosing the full path of the SurgeLDAP Server installation directory
- 2) CSS (Cross Site Scripting)
- 3) Denial of service
- 4) Clear text password storage

Path disclosure:

By requesting a file that does not exist on the server, for example

Securiteam: [NT] SurgeLDAP Multiple Security Vulnerabilities

<http://127.0.0.1:6680/aaa.html> it is possible to cause the server to return the path under which the product is installed.

CSS:

At least one of the parameters parsed by the product's CGIs allows remote attackers to insert malicious HTML and/or JavaScript into pages.

Exploit:

[http://127.0.0.1:6680/user.cgi?cmd=<script>alert\('C.S.S'\)</script>&utoken=](http://127.0.0.1:6680/user.cgi?cmd=<script>alert('C.S.S')</script>&utoken=)

Denial of service vulnerability:

A remote user can issue an HTTP GET request for a large amount of characters (e.g. '/AAAAA[501 times]'), causing the server crash.

Clear Text Password Storage Vulnerability:

SurgeLDAP Server stores usernames and passwords in a file called C:\surgedap\user.dat, the data stored there is in clear text.

Vendor response:

First of all thanks for bringing the below issues to my attention. :-)

> 1) *Disclosing the full path of the SurgeLDAP Server installation directory.*

Thanks, I have now updated it now says:

File Not Found (aaa.html)
or File Not Found (test\aaa.html)
..etc.

> 2) *CSS (Cross Site Scripting) .*
> 3) *Denial of service vulnerability .*

For these two one the site is all and ready I expect that end users would turn off the Web Server side of SurgeLDAP.

I have also just finished the capability to limit access to the modules by IP as well.

We also have plans to implement

- 1) insure password guessing is not allowed (e.g. limit guesses per ip per time)
- 2) have a setting to 'ignore' requests if they exceeds a certain rate per ip per time.
- 3) limit concurrent connections per ip, if limit exceeded drop links as they come in.

> 4) *Clear Text Password Storage Vulnerability .*

This one I have just finished updated yesterday, you can now save passwords using:

Securiteam: [NT] SurgeLDAP Multiple Security Vulnerabilities

plain text, ssha, sha, crypt or MD5.

Requires 1 change to the schema to select your wanted encoding method. :-)

ADDITIONAL INFORMATION

The information has been provided by <mailto:vulncode@yahoo.com> Ziv Kamir.

=====

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.