

NT2K systems dying, LsaSrv EventID 5000

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-06/0021.html>

From: David Soussan (*das_at_DASCOMPUTERCONSULTANTS.COM*)

Date: 06/06/05

Date: Mon, 6 Jun 2005 08:23:28 -0400
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Greetings;

Summary: Someone is testing a new exploit, most likely one fixed by MS04-11 though Microsoft should confirm this sometime today. If you have an NT2K machine with IIS running open on port 80 facing the internet and have not patched your system, you will most likely see this exploit knock on your front door.

Prior to 6/1/05, the MS04-11 holes were not exploited via port 80 & IIS.

Details:

Windows Server 2000 / SP4 / not fully security patched is affected.
Windows Server 2000 / SP4 / fully security patched – not yet known (I've been waiting patiently for the offending packet to re-arrive, but whoever was testing this exploit stopped for awhile)
Windows Server 2003 / IIS 6.0 is not affected.

The attack vector is via an IIS packet which calls for authentication, hands it a whole lot of data, and crashes LsaSrv that instant. Requires a server reboot to bring the 2K Server back online.

I've captured the offending packets and turned them over to Microsoft awaiting analysis.

How to know if you've been hit:

The crash event in the event log follows:

Event Type: Error
Event Source: LsaSrv
Event Category: Devices
Event ID: 5000
Date: 6/3/2005
Time: 7:38:06 AM
User: N/A
Computer: <your server name here>

NT-Bugtraq: NT2K systems dying, LsaSrv EventID 5000

Description:

The security package Negotiate generated an exception. The package is now disabled. The exception information is the data.

Data:

```
0000: 05 00 00 c0 00 00 00 00 .....
0008: 00 00 00 00 18 f2 55 78 .....Ux
0010: 02 00 00 00 00 00 00 00 .....
0018: 0c 00 00 00 3f 00 01 00 ...?...
0020: 00 00 00 00 00 00 00 00 .....
0028: 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 .....
0038: 7f 02 ff ff 00 00 ff ff ...
0040: ff ff ff ff 00 00 00 00 ....
0048: 00 00 00 00 00 00 00 00 .....
```

At the exact same date / time LsaSrv died, a log entry in the IIS logs that looks something like this:

(assuming MS IIS log format, yours might differ)

```
66.54.153.162, -, 6/3/2005, 7:38:06, W3SVC1, SERVER-E, 192.168.1.2, 110,
5699, 1 82, 500, 2148074244, GET, /, -,
```

The error code back from IIS of 2148074244 is not right. The inbound packet size of 5699 is a key indicator this exploit has knocked on your front door.

Note: This is for the variant of the exploit that was being tested late last week and crashes LsaSrv. I believe (but have no hard data to verify) this was someone testing an exploit that didn't quite work, causing the crash. He/She is probably fixing this so the exploit is more useful. So if you are curious if you've seen this exploit knock on your door, search your logs for the 5699 incoming packet size.

I believe we're seeing the field testing of a new exploit. The input vector is via a public facing IIS port 80. The packet gets IIS to try and do an SNMPv2-SMI::security.5.2 authentication (AKA: "SPNEGO - Simple Protected Negotiation") When the oversized packet (it is filled with "AAAAAAA...AAAA" to pad the buffer out) is handed around to various windows processes, apparently that overflows a buffer and does some other damage. I'm not sure what that other damage is --- there are some responses in various newsgroups where some people are saying they've got other processes running on their system now.

More to come as I find out.

David Soussan

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--