

[VulnWatch] SPIKE 2.5 and associated vulns

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-08/0008.html>

From: Dave Aitel (dave@immunitysec.com)

Date: 08/06/02

From: Dave Aitel <dave@immunitysec.com>

To: webappsec@securityfocus.com, bugtraq@securityfocus.com, pen-test@securityfocus.com, vuln-dev@securityfocus.com

Date: 05 Aug 2002 20:02:44 -0400

SPIKE 2.5 is now available at <http://www.immunitysec.com/spike.html>

This release (see the "audits" directory) includes:

- o one new remotely exploitable pre-auth bug on all versions of Microsoft SQL Server. I call it the "Hello" bug as in "You had me at hello" since the overflow occurs during the first possible opportunity. For reference, the bug itself is on TCP port 1433, and is a remote SYSTEM bug in the default configurations tested. There are some restrictions on the process's access token, but this is easily taken care of in many ways.

- o Several new vulnerabilities in Microsoft Exchange 2000
 - o 2 remote unauthenticated Access Violations via MSRPC (kills the MTA, may be remotely exploitable, but I haven't looked into it)
 - o 1 vulnerability in the MSRPC endpoint for the MTA that uses all available memory and sometimes bluescreens the box. This vulnerability is also unauthenticated, and also may be exploitable. You can use dcedump (now included with SPIKE) to locate the port the MTA endpoints are on.
 - o 1 post-auth vulnerability – rapid requests from an authenticated user will quickly exhaust the licenses granted by IIS to the Exchange server and cause the service to become unavailable until IIS and Exchange 2000 are restarted.

In addition, this release contains SPIKE Proxy 1.1.1 (minor bugfix release over 1.1 – GET /file.ext/arg=variable is now treated properly), updated SPIKE msprcfuzz and "generic" support, and many other bugfixes.

Dave Aitel
Immunity, Inc
<http://www.immunitysec.com/>

(Credit goes to someone in eEye for the clever name for the SQL server bug, if I recall correctly. It was a busy party and I forget exactly who told me that joke, which I shamelessly used during my BlackHat talk.)

- application/pgp-signature attachment: This is a digitally signed message part
-

- ***Previous message:*** Florian Weimer: "[VulnWatch] RUS-CERT Advisory 2002-08:02: Flaw in calloc and similar routines"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]