

KPMG-2002010: Microsoft IIS .htr ISAPI buffer overrun

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0137.html>

From: Peter Gründl (pgrundl@kpmg.dk)

Date: 04/11/02

From: Peter Gründl <pgrundl@kpmg.dk>
To: "bugtraq" <bugtraq@securityfocus.com>
Date: Thu, 11 Apr 2002 12:09:26 +0200

-->Microsoft IIS .htr ISAPI buffer overrun<==
courtesy of KPMG Denmark

BUG-ID: 2002010

CVE: CAN-2002-0071

Released: 11th Apr 2002

Problem:

=====

There is a buffer overrun condition in the isapi extension that handles .htr extensions that could allow an attacker to crash the service and possibly execute arbitrary code on the server.

Vulnerable:

=====

- Microsoft Internet Information Server 4.0
- Microsoft Internet Information Server 5.0

Details:

=====

This vulnerability was discovered by Dave Aitel from @stake and by Peter Gründl from KPMG. It was done independently, and both reported the same two vulnerabilities to the same vendor at around the same time.

Dave Aitel released an advisory on this issue:

<http://archives.neohapsis.com/archives/bugtraq/2002-04/0114.html>

Ism.dll handles files with the extension .htr and a flaw in the module could allow an attack to disable parts of or all of the functionality of a website. It is theoretically possible to execute code with this overflow, although attempted exploitation

SecurityFocus Bugtraq: KPMG-2002010: Microsoft IIS .htr ISAPI buffer overrun

would most likely result in a Denial of Service situation.

The problem is with the modules parameter handling, as declared variables are subject to a buffer overrun ("/foo.htr?<buffer>=x"). The number of overflows needed and the result depends on the internal state of the IIS memory allocations. A determined attacker could proceed to crash the service, and repeatedly send the malicious payload as the injection vector would now be relatively fixed, when the server was rebooted.

Vendor URL:

=====

You can visit the vendors webpage here: <http://www.microsoft.com>

Vendor response:

=====

The vendor was contacted on the 31st of January, 2002. On the 18th of March we received a private hotfix, which corrected the issue. On the 10th of April, the vendor released a public bulletin.

Corrective action:

=====

The vendor has released a patched ism.dll, which is included in the security rollup package MS02-018, available here: <http://www.microsoft.com/technet/security/bulletin/ms02-018.asp>

Author: Peter Gründl (pgrundl@kpmg.dk)

KPMG is not responsible for the misuse of the information we provide through our security advisories. These advisories are a service to the professional security community. In no event shall KPMG be liable for any consequences whatsoever arising out of or in connection with the use or spread of this information.

- **Previous message:** [Peter Gründl: "KPMG-2002009: Microsoft IIS W3SVC Denial of Service"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)