

Microsoft Security Bulletin MS01-044

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-08/0216.html>

From: Microsoft Product Security (secnotif@MICROSOFT.COM)

Date: 08/16/01

Message-ID: <2E08A46FF518C9418713A1B2C780684D103CFE@red-msg-20.redmond.corp.microsoft.com>
Date: Wed, 15 Aug 2001 19:49:56 -0700
From: Microsoft Product Security <secnotif@MICROSOFT.COM>
Subject: Microsoft Security Bulletin MS01-044
To: MICROSOFT_SECURITY@ANNOUNCE.MICROSOFT.COM

The following is a Security Bulletin from the Microsoft Product Security Notification Service.

Please do not reply to this message, as it was sent from an unattended mailbox.

-----BEGIN PGP SIGNED MESSAGE-----

Title: 15 August 2001 Cumulative Patch for IIS
Date: 15 August 2001
Software: IIS 4.0 and 5.0
Impact: Five vulnerabilities resulting in either denial of
service or privilege elevation
Bulletin: MS01-044

Microsoft encourages customers to review the Security Bulletin at:
<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>.

Issue:

=====

This patch is a cumulative patch that includes the functionality of all security patches released to date for IIS 5.0, and all patches released for IIS 4.0 since Windows NT(r) 4.0 Service Pack 5. A complete listing of the patches superseded by this patch is provided below, in the section titled "Additional information about this patch". Before applying the patch, system administrators should take note of the caveats discussed in the same section.

In addition to including all previously released security patches, this patch also includes fixes for five newly discovered security

vulnerabilities affecting IIS 4.0 and 5.0:

- A denial of service vulnerability that could enable an attacker to cause the IIS 4.0 service to fail, if URL redirection has been enabled. The "Code Red" worm generates traffic that can in some cases exploit this vulnerability, with the result that an IIS 4.0 machine that wasn't susceptible to infection via the worm could nevertheless have its service disrupted by the worm.
- A denial of service vulnerability that could enable an attacker to temporarily disrupt service on an IIS 5.0 web server. WebDAV doesn't correctly handle particular type of very long, invalid request. Such a request would cause the IIS 5.0 service to fail; by default, it would automatically restart.
- A denial of service vulnerability involving the way IIS 5.0 interprets content containing a particular type of invalid MIME header. If an attacker placed content containing such a defect onto a server and then requested it, the IIS 5.0 service would be unable to serve any content until a spurious entry was removed from the File Type table for the site.
- A buffer overrun vulnerability involving the code that performs server-side include (SSI) directives. An attacker who had the ability to place content onto a server could include a malformed SSI directive that, when the content was processed, would result in code of the attacker's choice running in Local System context.
- A privilege elevation vulnerability that results because of a flaw in a table that IIS 5.0 consults when determining whether a process should in-process or out-of-process. IIS 5.0 contains a table that lists the system files that should always run in-process. However, the list provides the files using relative as well as absolute addressing, with the result that any file whose name matched that of a file on the list would run in-process.

In addition, this patch eliminates a side effect of the previous IIS cumulative patch (discussed in the Caveats section of Microsoft Security Bulletin MS01-026) by restoring proper functioning of UPN-style logons via FTP and W3SVC.

Mitigating Factors:

=====

URL Redirection denial of service:

- This vulnerability only affects IIS 4.0. IIS 5.0 is not affected.
- The vulnerability only occurs if URL redirection is enabled.
- The vulnerability does not provide any capability to compromise data on the server or gain administrative control over it.

WebDAV request denial of service:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- The effect of an attack via this vulnerability would be temporary. The server would automatically resume normal service as soon as the malformed requests stopped arriving.

SecurityFocus Bugtraq: Microsoft Security Bulletin MS01-044

- The vulnerability does not provide an attacker with any capability to carry out WebDAV requests.
- The vulnerability does not provide any capability to compromise data on the server or gain administrative control over it.

MIME header denial of service:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

SSI privilege elevation vulnerability:

- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

System file listing privilege elevation vulnerability:

- The vulnerability only affects IIS 5.0. IIS 4.0 is not affected.
- In order to exploit this vulnerability, the attacker would need to have the ability to install content on the server. However, by default, unprivileged users do not have this capability, and best practices strongly recommend against granting it to untrusted users.

Patch Availability:

=====

- A patch is available to fix these vulnerabilities. Please read the Security Bulletin <http://www.microsoft.com/technet/security/bulletin/ms01-044.asp> for information on obtaining this patch.

Acknowledgment:

=====

- John Waters of Deloitte and Touche for reporting the MIME type denial of service vulnerability.
- The NSFocus Security Team (<http://www.nsfocus.com>) for reporting the SSI privilege elevation vulnerability.
- Oded Horovitz of Entercept(tm) Security Technologies (<http://www.entercept.com>) for reporting the system file listing privilege elevation vulnerability.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT

SecurityFocus Bugtraq: Microsoft Security Bulletin MS01-044

SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.1

```
iQEVAwUBO3s01I0ZSRQxA/UrAQEEuAgArZwsII6st0LxXkCCj6Z02o5EaISfDYrY
5zURDIKDzvaBv6UnQR5DmXix35O7vhge5HLUweF2bhfk9gsi+wAgq7I/zP0UNBC0
rHGnCVwtylbnlsXtm/kjKbd/+9vHpsjvegvMtARBAQJEBde0DMZUvblqBSLOSi3/
JPB7oNQ0A/Jsx5dfGBC8Tb7In0A5RC11Sk5rjdGUcOhy6Lh1Hrp50xpzEHyAH6r5
ORFY6h2X4rY+/yLlfefFL1FICMspDN6GoYXEWKhsxdJZPqXLR3VVUB1A4NyPhJ/
bQXfwqXNC4n0MOB8XIPpC2QtLinyD1+JrgK23L8eHTSx1ot5ouVEqQ==
=RVKU
```

-----END PGP SIGNATURE-----

You have received this e-mail bulletin as a result of your registration to the Microsoft Product Security Notification Service. You may unsubscribe from this e-mail notification service at any time by sending an e-mail to MICROSOFT_SECURITY-SIGNOFF-REQUEST@ANNOUNCE.MICROSOFT.COM. The subject line and message body are not used in processing the request, and can be anything you like.

To verify the digital signature on this bulletin, please download our PGP key at <http://www.microsoft.com/technet/security/notify.asp>.

For more information on the Microsoft Security Notification Service please visit <http://www.microsoft.com/technet/security/notify.asp>. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site at <http://www.microsoft.com/security>.

-
- **Previous message:** [Jim Paris: "Re: HTML Form Protocol Attack"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)