

Securiteam: [NT] Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

## [NT] Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0039.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/13/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Oct 2004 15:33:00 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

---

### SUMMARY

A denial of service vulnerability exists that could allow an attacker to send a specially crafted WebDAV request to a server that is running IIS and WebDAV. An attacker could cause WebDAV to consume all available memory and CPU time on an affected server. The IIS service would have to be restarted to restore functionality.

### DETAILS

Vulnerable Systems:

\* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D2C632A7-CD43-466C-A624-D841905CE181>>

Download the update

\* Microsoft Windows XP and Microsoft Windows XP Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6A338C59-3693-4A25-B823-431A5C21A4B7>>

Download the update

\* Microsoft Windows XP 64-Bit Edition Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0412A361-28C5-45F7-9853-BCDC9D7B2B97>>

Download the update

## Securiteam: [NT] Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

\* Microsoft Windows XP 64-Bit Edition Version 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1F9CA027-B0B8-47DC-BB96-8709E3DB0DF2>>

Download the update

\* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=81CE104D-5257-447C-A2CD-D4D149581D71>>

Download the update

\* Microsoft Windows Server 2003 64-Bit Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1F9CA027-B0B8-47DC-BB96-8709E3DB0DF2>>

Download the update

### Immune Systems:

\* Microsoft Windows XP Service Pack 2

\* Microsoft Windows NT Server 4.0 Service Pack 6

\* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

\* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

### Affected Components:

\* Internet Information Services 5.0

\* Internet Information Services 5.1

\* Internet Information Services 6.0

### Non-Affected Components:

\* Internet Information Server 4.0

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0718>>

CAN-2003-0718

### Mitigating Factors for WebDAV Vulnerability

\* The vulnerability can only be exploited remotely if an attacker can establish a Web session with an affected server.

\* By default, Windows XP and Windows Server 2003, except for Windows Server 2003 Web Server Edition, do not install IIS.

\* IIS 5.0, which is included as part of Windows 2000, is the only version that enables WebDAV by default.

### Workarounds for WebDAV Vulnerability

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified below.

\* Disable WebDAV on IIS 5.0 if it is not needed.

### FAQ for WebDAV Vulnerability

What is the scope of the vulnerability ?

This is a denial of service vulnerability. An attacker who successfully exploited this vulnerability could cause WebDAV to consume all available memory and CPU time on an affected server. The IIS service would have to be restarted to restore functionality.

## Securiteam: [NT] Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

What causes the vulnerability ?

WebDAV does not limit the number of attributes that can be specified per XML-element in WebDAV requests.

Why does this vulnerability require an upgrade to MSXML 3.0 Service Pack 5, which is included in this security update ?

The Microsoft XML Parser is a core operating system component that applications use to process XML documents. This component is used by WebDAV and by third-party applications. This update is required to allow WebDAV to limit the number of attributes that it can try to process on submitted documents.

Do I need to install MSXML 3.0 Service Pack 5 separately ?

No. The update package includes both the update for WebDAV and the upgrade files for MSXML 3.0 to upgrade your installation to Service Pack 5.

What is WebDAV ?

WebDAV is an industry standard extension to the HTTP specification. The \u201cDAV\u201d in \u201cWebDAV\u201d stands for \u201cdistributed authoring and versioning.\u201d WebDAV adds a capability for authorized users to remotely add and manage content on a Web server. By default, WebDAV is enabled when IIS is enabled on Windows 2000. By default, WebDAV is not installed on IIS 5.1 or on IIS 6.0.

What is wrong with the way that WebDAV handles HTTP requests ?

Before the recent update of the XML Parser, MSXML 3.0, WebDAV, or other third-party applications that use the Microsoft XML Parser, could not limit the number of attributes that the Microsoft XML Parser would try to process on submitted documents.

What might an attacker use the vulnerability to do ?

This is a denial of service vulnerability. An attacker could cause a disruption of normal services. Restarting the affected service restores normal functionality to the server. However, the service remains susceptible to a new denial of service attack until the update is applied.

Who could exploit the vulnerability ?

Any user who could deliver a WebDAV request to an affected Web server could exploit the vulnerability. Because WebDAV requests travel over the same port as HTTP (typically port 80), an attacker who could establish a connection to an affected Web server could try to exploit the vulnerability.

How could an attacker exploit the vulnerability ?

To exploit this vulnerability, an attacker would have to send a specially-crafted HTTP messages to an affected Web site that could increase the CPU utilization on the IIS server to 100% while IIS was processing the message. The more XML attributes contained per XML element in the XML message, the longer the IIS server would take to process the XML message. This could cause a denial of service while IIS is processing the messages and the service would have to be restarted to restore

Securiteam: [NT] Vulnerability in WebDAV XML Message Handler DoS (MS04-030)

functionality to the server.

What systems are primarily at risk from the vulnerability ?

Servers that are running both IIS and WebDAV services are primarily at risk from this vulnerability.

Could the vulnerability be exploited over the Internet ?

Yes. An attacker may be able to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information on how you can help protect your PC. End users can visit the <<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site. IT Professionals can visit the <<http://go.microsoft.com/fwlink/?LinkId=21171>> Security Guidance Center Web site.

What does the update do ?

The update removes the vulnerability by updating WebDAV to use the new XML parser properties to limit the number of XML attributes per element in the XML documents it accepts in WebDAV-based requests.

When this security bulletin was issued, had this vulnerability been publicly disclosed ?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-030.msp>>  
<http://www.microsoft.com/technet/security/bulletin/MS04-030.msp>

=====

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.