

[NT] Microsoft Exchange Server 2000 IMAP Literal Processing DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00017.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 9 May 2007 10:52:00 +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>

Microsoft Exchange Server 2000 IMAP Literal Processing DoS Vulnerability

SUMMARY

Microsoft Exchange Server 2000 is "a messaging product developed by Microsoft, part of the Windows Server System line of server products". Remote exploitation of an integer overflow vulnerability in the IMAP service of Microsoft Exchange 2000 could allow a remote attacker to crash all running Exchange services and other services in the same process.

DETAILS

Vulnerable Systems:

- * Microsoft Exchange 2000 with Service Pack 3

The vulnerability specifically exists in code responsible for reading of literals in the IMAP4 service. When the IMAP4 service encounters a specially crafted literal, it fails to properly process it. An access violation occurs causing an unhandled exception that terminates the process.

Analysis:

Exploitation of this vulnerability allows an attacker to cause the

[NT] Microsoft Exchange Server 2000 IMAP Literal Processing DoS Vulnerability

affected server to restart or potentially require data to be reinstalled from backup.

As the Exchange server may run in the same process space as many other servers, crashing the IMAP4 component will also cause the SMTP, POP3, WWW and FTP services, if enabled, to exit. In order to exploit this vulnerability, the attacker must have access to establish a TCP session with the IMAP4 service.

Vendor response:

Microsoft has addressed this vulnerability within MS07-026. For more information, consult their bulletin at the following URL:

<http://www.microsoft.com/technet/security/Bulletin/MS07-026.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS07-026.mspx>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0221>
CVE-2007-0221

Disclosure timeline:

01/10/2007 – Initial vendor notification
01/22/2007 – Initial vendor response
05/08/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<mailto:idlabs-advisories@xxxxxxxxxxxxx> iDefense Labs Security Advisories.

The original article can be found at:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=526>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=526>

=====

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@xxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

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.