

[NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/19/03

To: list@securiteam.com

Date: 19 Oct 2003 12:08:36 +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 Exchange Server Could Allow Arbitrary Code Execution
(MS03-046)

SUMMARY

In Exchange Server 5.5, a security vulnerability exists in the Internet Mail Service that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted extended verb request that could allocate a large amount of memory. This could shut down the Internet Mail Service or could cause the server to stop responding because of a low memory condition.

DETAILS

Vulnerable Systems:

- * Microsoft Exchange Server 5.5, Service Pack 4
- * Microsoft Exchange 2000 Server, Service Pack 3

Immune Systems:

- * Microsoft Exchange Server 2003

Patch Availability:

*

Securiteam: [NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A9E872EA-54B0-4179-8AE9-5648BFB46459&disp>>
Microsoft Exchange Server 5.5, Service Pack 4

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7BAF5394-1B4E-4937-A570-9F232AE49F01&disp>>
Microsoft Exchange 2000 Server, Service Pack 3

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0714>>
CAN-2003-0714

In Exchange 2000 Server, a security vulnerability exists that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted extended verb request. That request could cause a denial of service that is similar to the one that could occur on Exchange 5.5. Additionally, if an attacker issues the request with carefully chosen data,