

Alert: Microsoft Security Bulletin MS05-034 – Cumulative Security Update for ISA Server 2000 (899753)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-06/0013.html>

From: Cooper, Russ (*russ.cooper_at_CYBERTRUST.COM*)

Date: 06/14/05

Date: Tue, 14 Jun 2005 13:41:01 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-034:
Cumulative Security Update for ISA Server 2000 (899753)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-034.msp>>

Version Number: 1.0

Issued Date: Tuesday, June 14, 2005

Impact of Vulnerability: Elevation of Privilege Maximum Severity Rating:
Moderate

Patch(es) Replaced: None

Caveats: None

Tested Software:

Affected Software:

* Microsoft Internet Security and Acceleration (ISA) Server 2000 Service Pack 2 Note The following software programs include ISA Server 2000. Customers who use these software programs should install the provided ISA Server 2000 security update.
– Microsoft Small Business Server 2000
– Microsoft Small Business Server 2003 Premium Edition ISA Server 2000 Service Pack 2, Small Business Server 2000, Small Business Server 2000 Service Pack 1, Small Business Server 2003 <<http://tinyurl.com/9dgcz>>

Technical Description:

* HTTP Content Header Vulnerability – CAN-2005-1215: A vulnerability exists in ISA Server 2000 because of the way that it handles malformed HTTP requests. An attacker could exploit the vulnerability by constructing a malicious HTTP request that could potentially allow an attacker to poison the cache of the affected ISA server. As a result, the attacker could either bypass content restrictions and access content that they would normally not have access to or they could cause users to

Alert: Microsoft Security Bulletin MS05-034 – Cumulative Security Update for ISA Server 2000 (899753)

be directed to unexpected content. Additionally, an attacker could use this in combination with a separate Cross Site Scripting vulnerability to obtain sensitive information such as logon credentials.

* NetBIOS Predefined Filter Vulnerability – CAN-2005-1216: An elevation of privilege vulnerability exists in ISA Server 2000 that could allow an attacker who successfully exploited this vulnerability to create a NetBIOS connection with an ISA Server by utilizing the NetBIOS (all) predefined packet filter. The attacker would be limited to services that use the NetBIOS protocol running on the affected ISA Server.

This email is sent to NTBugtraq automagically as a service to my subscribers. (v4.01.1975.38886)

Cheers,
Russ Cooper – Senior Scientist – Cybertrust/NTBugtraq Editor

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--