

# [NT] Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0062.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/23/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 23 Mar 2003 12:32:47 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service

---

## SUMMARY

Microsoft Internet Security and Acceleration (ISA) Server 2000 contains the ability to apply application filters to incoming traffic. Application filters allow ISA Server to analyze a data stream for a particular application and provide application-specific processing including inspecting, screening or blocking, redirecting, or modifying the data as it passes through the firewall. This mechanism is used to protect against invalid URLs that may indicate attempted attacks as well as attacks against internal Domain Name Service (DNS) Servers.

A flaw exists in the ISA Server DNS intrusion detection application filter, and results because the filter does not properly handle a specific type of request when scanning incoming DNS requests.

An attacker could exploit the vulnerability by sending a specially formed request to an ISA Server computer that is publishing a DNS server, which could then result in a denial of service to the published DNS server. DNS

## Securiteam: [NT] Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service

requests arriving at the ISA Server would be stopped at the firewall, and not passed through to the internal DNS server. All other ISA Server functionality would be unaffected.

### DETAILS

#### Affected Software:

- \* Microsoft ISA Server

#### Mitigating factors:

- \* By default, no DNS servers are published. DNS server publishing must be manually enabled.
- \* The vulnerability would not enable an attacker to gain any privileges on an affected ISA Server or the published DNS server or to compromise any cached content on the server. It is strictly a denial of service vulnerability.

#### Patch availability:

Download locations for this patch Microsoft ISA Server:

- \* English:

<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=en>  
<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=en>

- \* French:

<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=fr>  
<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=fr>

- \* German:

<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=de>  
<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=de>

- \* Spanish:

<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=es>  
<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=es>

- \* Japanese:

<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=ja>  
<http://microsoft.com/downloads/details.aspx?FamilyId=F62127C5-51E3-4B34-A6D3-B9CF840358BD&displaylang=ja>

What's the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who successfully exploited this vulnerability could cause an ISA Server to stop sending incoming Domain Name Service (DNS) requests to a published DNS server. Restarting the ISA Server service would allow DNS server publishing and DNS intrusion detection to function correctly again; however, the server

## Securiteam: [NT] Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service

would remain vulnerable to another denial of service attack.

Could an attacker use the vulnerability to take control of an ISA Server computer?

No. This is a denial of service attack only. There is no capability to usurp any administrative privileges.

Could an attacker use the vulnerability to breach the security of the firewall?

No. There is no capability to use this vulnerability to lower the security the firewall provides. It can only be used to prevent the ISA Server from passing any further DNS requests to the published DNS server.

Could an attack that attempted to exploit this vulnerability be launched from the Internet?

Yes, the specially formed request could be sent from the Internet to a computer running ISA Server.

What is ISA Server?

ISA Server provides both an enterprise firewall and a high-performance web cache. The firewall protects the network by regulating which resources can be accessed through the firewall, and under what conditions. The web cache helps improve network performance by storing local copies of frequently requested web content.

What is Domain Name Service (DNS)?

Domain Name Service (DNS) is a service that resolves a domain name to an IP address. For instance, a client computer wishing to visit the website <http://www.microsoft.com> must first resolve the domain name "microsoft.com" to its Internet IP address. This is done by contacting a DNS server.

What is DNS server publishing?

DNS server publishing allows an administrator to configure ISA Server to send DNS name resolution requests from an external network to an organization's internal DNS server.

What is the DNS intrusion detection filter?

When configured for DNS server publishing, the DNS intrusion detection filter scans incoming DNS requests before they are passed on to an internal DNS server for processing. This filter scans incoming requests to protect against certain forms of remote attack.

What's wrong with ISA Server's DNS intrusion detection filter?

The DNS intrusion detection filter does not correctly handle a particular type of DNS request under a specific circumstance. If such a request were received, it could cause the DNS server-publishing feature to stop responding. Normal intrusion detection of other requests and all other ISA Server operations would be unaffected.

Securiteam: [NT] Flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service

How great a threat does this vulnerability pose?

It depends on whether DNS server publishing feature is enabled. By default, it is disabled. However, if it were enabled, any Internet user could potentially exploit this vulnerability to cause the DNS server-publishing feature to stop responding. DNS requests received after the occurrence of a successful exploit would be stopped at the firewall and would not pass into the network.

What does the patch do?

The patch eliminates the flaw by ensuring the DNS intrusion detection filter properly processes DNS requests.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0\_45731\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\_US@Newsletters.Microsoft.com>  
Microsoft Product Security.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.