Cisco Small Business Routers.

RVS4000 and WRVS4400N IPS Signature Release Note

Version: 1.41 Total Rules: 1098

In this signature, we addressed the exploits/vulnerabilities and applications as below:

-EXPLOIT MS Video ActiveX Control Stack Buffer Overflow
A buffer overflow vulnerability exists in Microsoft DirectShow.
The flaw is due to the way Microsoft Video ActiveX Control parses image files.
An attacker can persuade the target user to open a malicious web page to exploit
this vulnerability.

-EXPLOIT Oracle Database Workspace Manager SQL Injection
Multiple SQL injection vulnerabilities exist in Oracle Database Server product.
The vulnerabilities are due to insufficient sanitization of input parameters
in the Oracle Workspace Manager component. A remote attacker with valid user
credentials may leverage these vulnerabilities to inject and execute SQL code
with escalated privilegesof SYS or WMSYS account.

Support P2P application named uTorrent up to version 1.7.2.

Signature content for 1.41
==========
New Added signature(s):
1053635 EXPLOIT MS Video ActiveX Control Stack Buffer Overflow -1
1053636 EXPLOIT MS Video ActiveX Control Stack Buffer Overflow -2
1053632 EXPLOIT Oracle Database Workspace Manager SQL Injection -1
1053633 EXPLOIT Oracle Database Workspace Manager SQL Injection -2
1053634 EXPLOIT Oracle Database Workspace Manager SQL Injection -3

Modified signature(s):
1051783 P2P Gnutella Connect
1051212 P2P Gnutella Get file
1051785 P2P Gnutella UDP PING 2
1051997 P2P Gnutella Bearshare file transfer with UDP
1052039 P2P Gnutella OK
1052637 P2P Foxy Get file

Deleted signature(s):
1050521 Worm.Klez.E1 - 1
1050522 Worm.Klez.E1 - 2
1050523 Worm.Klez.E1 - 3
1050524 Worm.Klez.E2 - 1
1050525 Worm.Klez.E2 - 2
1050526 Worm.Klez.E2 ¡V 3
1050536 Worm.Blaster.B - 1
1050537 Worm.Blaster.B - 2
1050538 Worm.Blaster.B - 3
1050539 Worm.Blaster.C - 1
1050540 Worm.Blaster.C - 2
1050541 Worm.Blaster.C - 3

Number of rules in each category:
==========
DoS/DDoS 51
Buffer Overflow: 241
Access Control: 92
Scan: 41
Trojan Horse: 62
Misc: 3
P2P: 40
Instant Messenger: 121
Vrus/Worm: 410
Web Attacks: 37

Version: 1.40 Total Rules: 1091

In this signature, we addressed the exploits/vulnerabilities and applications as below:

1053406 EXPLOIT MS IE HTML Embed Tag Stack Buffer Overflow (CVE-2008-4261)
A boundary error when processing an overly long filename extension specified inside an "EMBED" tag can be exploited to cause a stack-based buffer overflow.

1053421 EXPLOIT MS IE XML Handling Remote Code Execution (CVE-2008-4844)
The vulnerability is caused due to a use-after-free error when composed HTML elements are bound to the same data source. This can be exploited to

dereference freed memory via a specially crafted HTML document

Version 1.38

In this signature, we addressed the following exploits/vulnerabilities and applications:

1. Support P2P applications, i.e. BitTorrent and eMule.

Version 1.33

In this signature, we addressed the following exploits/vulnerabilities and applications:

1. Support IM application named AIM (http://dashboard.aim.com/aim) up to version 6.5.

2. Support IM application named MSN (http://get.live.com/messenger) up to version 8.1.

3. PcShare is a trojan tool, which can remotely administer an attacked PC.

4. CVE-2007-3039: The vulnerability is caused by a boundary error in the Microsoft Message Queueing service (MSMQ) when processing MSMQ messages.
   This can be exploited to cause a buffer overflow by sending specially crafted packets to the MSMQ service.

Version 1.32

In this signature, we addressed the following peer-to-peer applications:

1. Support IM application named AIM up to version 6.5.
2. Support IM application named MSN up to version 8.1.

Version 1.31

In this signature, we addressed the following peer-to-peer applications:

1. Support P2P application named BitTorrent up to version 5.0.8.

2. Support P2P application named uTorrent up to version 1.7.2.

Version 1.30

In this release, we addressed the following vulnerabilities in Microsoft applications:

1. BID-24462: A Null dereference vulnerability exists in certain versions of Microsoft Office. Remote attackers can trick users to visit a specially crafted web page. The symptom includes a denial of service condition to the affected process.

2. Microsoft Security Bulletin MS07-027: The Microsoft Windows Media Services NMSA Session Description Object ActiveX control fails to restrict access to dangerous methods. This vulnerability could allow a remote attacker to execute arbitrary code on an affected system.

Version 1.29

In this release, we addressed the following exploits/vulnerabilities and peer-to-peer applications:

1. Microsoft Security Advisory(935423): There exists a stack-based buffer overflow in Microsoft Windows. The vulnerability is due to insufficient format validation while handling malformed ANI cursor or icon files. A remote attacker can exploit this vulnerability by enticing the target user through visit a malicious website using Internet Explorer. Successful exploitation would allow for arbitrary code execution with the privileges of the currently logged-in user.

2. Support blocking an Instant Messaging application named QQ up to version 2007 Beta1 and Beta2.

Version 1.28

In this signature, we address the following exploits/vulnerabilities:

Microsoft Security Bulletin MS07-014: There exists a buffer overflow vulnerability in Microsoft Word. The vulnerability is created due to a flaw in the Section Table entry inside the Table Stream structure.

An attacker may exploit this vulnerability by enticing a user to open a crafted Word file. Exploitation of the vulnerability may result in injection and execution of arbitrary code within the security context of the target user.

Microsoft Security Bulletin MS07-016: There exists a memory corruption vulnerability in Microsoft Internet Explorer. The flaw is due to improper validation of reply lines in FTP server responses. By persuading a user to visit a malicious web site, an attacker may execute arbitrary code on the target system with the privileges of the currently logged on user.

Version 1.26

In this signature, we addressed the following exploits/vulnerabilities:

CVE-2006-5559: There exists a memory corruption vulnerability in the ADODB.Connection ActiveX control in Microsoft Internet Explorer. The flaw is due to improper validation of data supplied to the execute method. By persuading the target user to visit a malicious web site, an attacker may cause the affected application process to terminate or possibly divert its execution flow to arbitrary code.

Version 1.25

In this signature, we addressed the following exploits/vulnerabilities:

Microsoft Security Bulletin MS06-070: MS Windows 2000 Workstation Service(WKSSVC.DLL) has a remote code execution vulnerability. An unauthenticated attacker could exploit this vulnerability to execute arbitrary code with system-level privileges on Windows 2000 and Windows XP machines.

Version 1.24

In this signature, we addressed the following exploits/vulnerabilities:

1. Microsoft Data Access Components (MDAC) has a remote code execution vulnerability in the RDS.Dataspace ActiveX control. A remote attacker could create a specially-crafted file and host the malicious file on a Web site or send it to the victim through email. When the file is opened, the attacker can execute arbitrary code on a victim's system.

2. The WMI Object Broker ActiveX control (WmiScriptUtils.dll) in Microsoft Visual Studio 2005 has a vulnerability, which could allow a remote attacker to execute arbitrary code.

3. Microsoft Internet Explorer has a Heap Buffer Overflow vulnerability. A remote attacker could creat a malicious web page containing COM objects Daxctle.OCX HTML when instantiation as an ActiveX control, and trick the victim to open the web page. By this attack, the attacker could execute arbitrary code on the victim's browser.

Version 1.23

In this release, we addressed the following exploits/vulnerabilities:

The vulnerability resides in some of the core XML engines in Microsoft Windows. It is the result of the engine's inability to properly handle improper arguments passed to one of the methods associated with the XML request object.

Version 1.22

In this release, we addressed the exploits/vulnerabilities as the following:

Vagaa is a P2P software which supports both eDonkey and BitTorrent network. It can be downloaded from both network. The software is mainly used in PRC. There are some issues about this software because it didn't follow formal eMule protocol.
The issue can be referenced on the wiki (http://en.wikipedia.org/wiki/Vagaa). We classify Vagaa as eDonkey2000 program and allow admin users to disable it in the Web UI.

Version: 1.21

In this release, we addressed the exploits/vulnerabilities as below:

Microsoft Internet Explorer WebViewFolderIcon has a Buffer Overflow Vulnerability. A remote attacker could create a malicious Web page and trick the victim to open. By this attack, the attacker could cause Buffer Overflow and crash the victim's browser.

Version: 1.20

In this release, we addressed the exploits/vulnerabilities and applications as below:

1. Foxy is an P2P application which can search and download music and movie. Foxy follows most of the public Gnutella P2P protocol but still has its own signature in some condition. After the inclusion of the P2P Foxy Get file rule we can fully detect and block Foxy and it will be detected as Gnutella. Foxy can be blocked by disabling Gnutella.

2. Microsoft Internet Explorer 6.0 and 6.0SP1 have a memory corruption vulnerability in the ActiveX component. A remote attacker could create a malicious Web page and trick the victim to open the web page. By this attack, the attacker could cause the victim's browser crash or execute arbitrary code.

3. Microsoft Internet Explorer has Heap Buffer Overflow vulnerabilities in Vector Markup Language (VML). A remote attacker could create a malicious Web page and trick the victim to open the web page. By this attack, the attacker could cause Buffer Overflow and execute arbitrary code on the victim's browser.

Version: 1.19

In this release, we added one rule to address the Redirect Cross-Domain Vulnerability (MS06-042) of Microsoft Internet Explorer. The vulnerability is caused by the improper handling of URL redirect by the object.documentElement.outer
HTML property. A remote attacker could create a malicious web page and trick the victim to open the web page. With this attack, the attacker could execute arbitrary code on the victim's browser and obtain sensitive information.

Version: 1.18

In this release, we added 6 rules to facilitate the blocking of QQ, the most popular instant messanger in China. There are many versions of QQ on the official website for download. Currently we can detect and block QQ up to the 2006 Beta2 Sp3 version.

Version: 1.17

In this release, we addressed the exploits/vulnerabilities below:

1. The Server Service in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 and SP1 have a buffer overflow vulnerability. A remote attacker could exploit a crafted Server response to cause buffer overflow and execute arbitrary code on the victim's system.

2. Hyperlink Object Library in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 and SP1 have a code execution vulnerability. A remote attacker could send a malicious Office document containing a specially crafted hyperlink to a victim in an email or host the file on a web site. When successfully exploiting this vulnerability, a remote attacker could execute arbitrary code with the victim's privileges.

3. Microsoft Word XP and Word 2003 have a remote code execution vulnerability. A remote attacker could host a malicious DOC file on a Web site. If successfully exploiting this vulnerability, the remote attacker could execute arbitrary code with the victim's privilege.

Version: 1.16

In this release, we addressed the exploits/vulnerabilities below:

1. Microsoft Excel 2000, XP and Excel 2003 have a remote code execution vulnerability, due to an error in Excel while handling malformed URL strings. A remote attacker could send a malicious .xls file to a victim in an email or host the file on a web site. When successfully exploiting this vulnerability, a remote attacker could execute arbitrary code with the victim's privileges.

2. Hyperlink Object Library in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 and SP1 have a code execution vulnerability. A remote attacker could send a malicious Office document containing a specially crafted hyperlink to a victim in an email or host the file on a web site. When successfully exploiting this vulnerability, a remote attacker could execute arbitrary code with the victim's privileges.

3. Microsoft Windows XP/NT/2000/2003 have a denial-of-service vulnerability. A remote attacker could send a malicious SMB packet to cause victim computers to crash.