

Cisco Applied Intelligence Response: Identifying and Mitigating Exploitation of the Microsoft Windows VML Arbitrary Code Execution Vulnerability

Document ID: 71712

<http://www.cisco.com/warp/public/707/cisco-air-20061004-ms-v>

Revision 1.0

For Public Release 2006 October 4 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)

[Cisco Intrusion Prevention System \(IPS\)](#)

[Cisco Security Agent \(CSA\)](#)

[Cisco Security Monitoring, Analysis, and Response System \(CS MARS\)](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

Cisco Response

Vulnerability Characteristics

The Microsoft Windows Vector Markup Language (VML) Arbitrary Code Execution vulnerability can be exploited remotely without authentication, and user interaction is necessary. Successful exploitation could allow the attacker to perform remote code execution with the privileges of the user or create a denial of service condition. The threat vector requires that the attacker entice the target user to view the malicious VML code, likely by means of social engineering. Common threat vectors include malicious web pages and malicious web-based e-mail. This vulnerability is designated by CVE ID CVE-2006-4868.

Vulnerability Overview

This document contains information to assist Cisco customers in mitigating attempts to exploit the Microsoft Windows VML arbitrary code execution vulnerability.

Server and desktop computing systems using the following Microsoft Windows operating systems are affected:

- Windows XP Service Pack 2 or prior
- Windows XP Professional x64 Edition
- Windows Server 2003 Service Pack 1 or prior
- Windows Server 2003 for Itanium-based Systems Service Pack 1 or prior

- Windows Server 2003 x64 Edition

Server and desktop computing systems using the following Microsoft Windows components are affected:

- Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4
- Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4

See the [Microsoft MS06–055 Bulletin](#) for full details.

Mitigation Technique Overview

Cisco devices provide countermeasures for the Microsoft Windows VML Arbitrary Code Execution vulnerability. The most preventive control is provided by the Cisco Security Agent (CSA) host intrusion prevention system software running in protect mode on the end host. CSA provides "Zero-Day" mitigation for all known threat vectors seen to date used by attacks in attempts of exploiting this vulnerability. Detective controls can be performed by the Cisco Intrusion Prevention System (IPS) product suite, which provides identification and protection starting with Signature Update S249 using signatures 5813/0 – 5813/3. Detective controls can also be performed by the Cisco Intrusion Detection System (IDS) product suite, which provides identification and protection starting with Signature Update S250 using signature 5813/0.

Device-Specific Mitigation and Identification

Specific information on mitigation and identification is available for these devices:

- [Cisco Intrusion Prevention System \(IPS\)](#)
- [Cisco Security Agent \(CSA\)](#)
- [Cisco Security Monitoring, Analysis, and Response System \(CS MARS\)](#)

Cisco Intrusion Prevention System (IPS)

Mitigation

The Cisco Intrusion Prevention System (IPS) provides detection and threat mitigation for the Microsoft Windows VML Arbitrary Code Execution [\(MS06–055\)](#) vulnerability starting with Cisco IPS Signature Update S249 for 5.x devices.

- Signature Update S249 (released September 20, 2006) – Added signatures 5813/0 – 5813/3
- Signature Update S250 (released September 21, 2006) – Added signature 5813/4
- Signature Update S251 (released September 26, 2006) – Modified signatures 5813/1 – 5813/3; Retired signature 5813/4
- Signature Update S253 (released October 3, 2006) – Modified signature 5813/3

The Cisco Intrusion Detection System (IDS) provides detection and threat mitigation for the Microsoft Windows VML Arbitrary Code Execution [\(MS06–055\)](#) vulnerability starting with Cisco IDS Signature Update S250 for 4.x devices.

- Signature Update S250 (released September 21, 2006) – Added signatures 5813/0

In order to trigger preventative controls, the IPS 5.x meta signature 5813/0 or the IDS 4.x signature 5813/0 will need to be configured to perform a response action. The actions that provide this type of mitigation are most effective when using an IPS device that is deployed in inline mode. Attacks attempting to exploit this vulnerability primarily use malicious web pages or malicious web based e-mails as the threat vector, thus attacks are TCP based and unlikely to be spoofed.

Identification

Cisco IPS 5.x meta signature 5813/0 and Cisco IDS 4.x signature 5813/0 trigger a High severity event upon the detection of an attempt to exploit the Microsoft Windows VML Arbitrary Code Execution. An IPS 5.x device triggered the following event using signature 5813/0 after an exploit attempt of this vulnerability on the target victim at IP address 192.0.2.1.

```
evIdsAlert: eventId=1142678274372769976 severity=high vendor=Cisco
  originator:
    hostId: sensor5x
    appName: sensorApp
    appInstanceId: 339
  time: 2006/09/28 15:06:01 2006/09/28 09:06:01 CST
  signature: description=Microsoft Internet Explorer Vector Markup Language Vulnerability
  subsigId: 0
  sigDetails: Microsoft Internet Explorer Vector Markup Language Vulnerability
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.0.2.254
      port: 80
    target:
      addr: locality=IN 192.0.2.1
      port: 1104
  triggerPacket:
  <TriggerPacket removed>
  riskRatingValue: 65
  interface: ge0_0
  protocol: tcp
```

Cisco Security Monitoring, Analysis, and Response System (CS MARS) (as shown below) and IPS/IDS Event Viewer (IEV) can be used to monitor for attempted exploitation of this vulnerability. Events produced when signature 5813/0 triggers indicate potential attempts to exploit this vulnerability and should be investigated.

Signature Summary

A number of signatures were defined in Signature Updates S249, S250, S251, and S253. Of these signatures, IPS 5.x customers should monitor for meta signature 5813/0 and IDS 4.x customers should monitor for signature 5813/0. IPS 5.x signatures 5813/1 – 5813/3 are the effective component signatures of meta signature 5813/0 that identify the steps during an attempt of exploiting this vulnerability.

Cisco Security Agent (CSA)

Mitigation

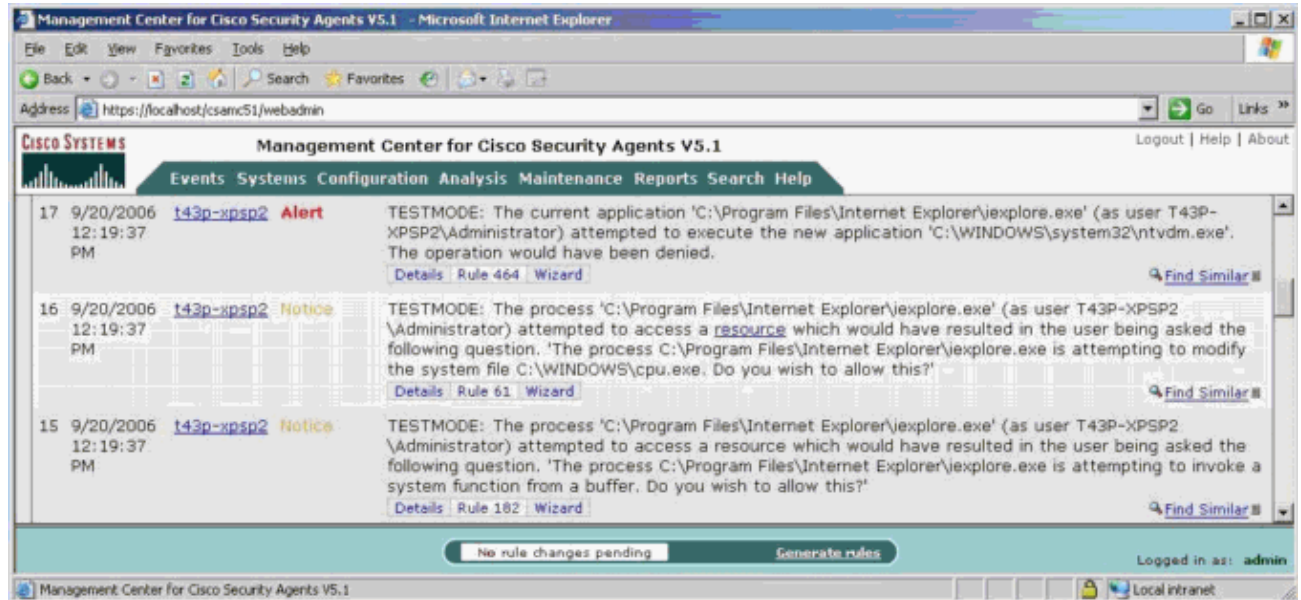
Current supported versions of Cisco Security Agent 4.0.3.x, 4.5.1.x, 5.0.0.x, and 5.1.0.x are effective in stopping all known exploits seen to date, thus providing "Zero-Day" protection at the end host. CSA host intrusion prevention system software effectively stops both the initial buffer overflow attempt and any subsequent steps to exploit the Microsoft Windows VML document arbitrary code execution vulnerability. The subsequent steps can include attempts to write the exploit's executable file into the **system32** directory and attempts by Internet Explorer to launch **NTVDM.exe**.

Note: These subsequent steps are only evident when running CSA in "Test Mode". When running CSA in "Protect Mode" (which is the recommended operating mode), the initial buffer overflow attempt is prevented and no further actions are executed by the exploit.

Note: For additional information on how CSA prevents exploitation of the MS06-055 vulnerability, please refer to [CSA Protects Against IE VML Buffer Overflow](#).

Identification

As shown in this example, the CSA Management Center (CSA MC) console can be monitored for attempts to exploit this vulnerability.



Cisco Security Monitoring, Analysis, and Response System (CS MARS)

Identification

As depicted in these examples, the CS MARS console can be monitored for attempts to exploit this vulnerability. Using the following query on the CS MARS appliance, events triggered by Signature 5813 will be displayed:

CISCO SYSTEMS

SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP

Query Batch Query Report Sep 28, 2006 2:28:31 PM EDT

QUERY / REPORTS | CS-MARS Standalone: MARS20-01 v4.2 Login: Administrator (pnadmin) :: Logout :: Activate

View Cases New Case

Load Report as On-Demand Query with Filter

Select Group... Incident ID: Show

Select Report... Session ID: Show

Query Event Data
Click the cells below to change query criteria:

Query type: Event Raw Messages ranked by Time, 1d-0h

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	IDSM2-rcdn	ANY	5813	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:1075148106, S:1075148106	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148106/1,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148116, S:1075148116	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148116/2,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148121, S:1075148121	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148121/3,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148126, S:1075148126	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075148126/1,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075148130, S:1075148130	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075148130/2,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075139649, S:1075139649	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139649/1,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139659, S:1075139659	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139659/2,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139664, S:1075139664	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139664/3,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139669, S:1075139669	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075139669/1,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075139673, S:1075139673	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075139673/2,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075126711, S:1075126711	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126711/1,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126721, S:1075126721	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126721/2,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126726, S:1075126726	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126726/3,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126731, S:1075126731	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075126731/1,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075126735, S:1075126735	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075126735/2,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1057		False Positive

The display shown here is the result of the previous query for IPS events triggered by Signature 5813:

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:1075148106, S:1075148106	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148106/1,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148116, S:1075148116	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148116/2,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148121, S:1075148121	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075148121/3,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075148126, S:1075148126	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075148126/1,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075148130, S:1075148130	Unknown Device Event Type [a]	Sep 27, 2006 5:05:28 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075148130/2,Time:1159391128,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075139649, S:1075139649	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139649/1,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139659, S:1075139659	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139659/2,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139664, S:1075139664	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075139664/3,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075139669, S:1075139669	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075139669/1,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075139673, S:1075139673	Unknown Device Event Type [a]	Sep 27, 2006 4:56:12 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075139673/2,Time:1159390572,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075126711, S:1075126711	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126711/1,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126721, S:1075126721	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126721/2,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126726, S:1075126726	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.66.89.11/80 --> 192.168.181.129/1104 TCP Unknown Device Event Type,NR:1075126726/3,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1104		False Positive
E:1075126731, S:1075126731	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075126731/1,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1057		False Positive
E:1075126735, S:1075126735	Unknown Device Event Type [a]	Sep 27, 2006 4:42:08 PM EDT	IDSM2-rcdn	10.68.36.124/80 --> 10.69.2.19/1057 TCP Unknown Device Event Type,NR:1075126735/2,Time:1159389728,Risk Rating:0,VLAN:0,Port List:1057		False Positive

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.0	2006–October–4	Initial public release.
--------------	----------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [IPS 5.x Signature Downloads](#) ([registered](#) customers only)
 - [IDS 4.x Signature Downloads](#) ([registered](#) customers only)
 - [Signatures by Release Version](#) ([registered](#) customers only)
 - [Cisco Systems IntelliShield Vulnerability Alert ID – 11738](#) (IntelliShield customers only)
 - [MySDN Report ID – 5156](#)
 - [Microsoft Security Bulletin MS06–055 \(925486\)](#)
 - [Microsoft Security Advisory \(925568\)](#)
 - [Cisco Security Agent \(CSA\)](#)
 - [Cisco Intrusion Prevention System \(IPS\)](#)
 - [Cisco Security Monitoring, Analysis and Response System \(CS MARS\)](#)
-

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Oct 04, 2006

Document ID: 71712
