

MWR InfoSecurity Security
Advisory

Sophos RMS / TAO
Component DoS
Vulnerability

16th January 2009

MWR  INFOSECURITY

Contents

1	Detailed Vulnerability Description	5
1.1	Introduction	5
1.2	Technical Background.....	5
1.3	Vulnerability Details.....	6
1.4	Vulnerability Impact.....	7
1.5	Exploit Information	7
1.6	Dependencies	7
2	Recommendations.....	8

Sophos RMS / TAO Component Denial of Service

Package Name:	Sophos Remote Management System / TAO Component
Date:	16 th January 2009
Affected Versions:	All versions of RMS before 3.0.9

CVE Reference	CVE-2009-0117
Author	M. Ruks
Severity	Low/Medium Risk
Local/Remote	Remote
Vulnerability Class	Denial of Service
Vendor Response	The vendor was contacted and worked with MWR InfoSecurity during the remediation process. Sophos have produced updated versions of their software to resolve the vulnerability. MWR InfoSecurity would like to thank Sophos for their assistance during this process.
Exploit Details Included	Yes (although no exploit code is provided)
Versions Affected	All versions up to but not including 3.0.9
Affected OS	All supported Operating Systems

Overview:

The Remote Management System (RMS) router component of Sophos Anti-Virus utilises TAO, which is a third party developed message request broker that contains a vulnerability. This RMS component is used by a service in installations of Sophos software. By constructing a specially crafted packet it is possible to cause the service to terminate. This attack could be performed without authenticating to the remote system.

Impact:

The vulnerability could enable an attacker to remotely disable the service without the need to provide valid credentials. This would prevent users within the organisation from managing the software although it will not prevent users from receiving malware definitions nor will it affect their level of protection. On operating systems with a Service Management feature the RMS router will restart after a given period; however, constantly sending a specific packet or targeting a non-managed Service (for example on Windows 9x and some UNIX platforms) will create a Denial of Service condition.

Cause:

The vulnerability arises from the interpretation of a length field within a GIOP packet passed to the service. This causes a memory allocation error within the TAO CORBA implementation, which does not handle the initial error correctly and is used by the RMS service. The error indicates that an out of memory error has occurred and therefore when this



is passed to the Sophos software it legitimately terminates its process as recovery from the error requires it to be restarted.

Interim Workaround:

One method for mitigating the risk associated with this issue is to use network filtering controls to protect the CORBA service, which runs on TCP port 8193. Communication with this TCP service is not required by the Sophos Enterprise Console or for endpoint communications and therefore can be protected by filtering controls. However, the correct resolution of the issue is recommended to fully mitigate the risk associated with it.

Solution:

The Sophos Anti-Virus software should be updated to the latest release; the issue has been resolved in RMS 3.0.9 and above. The following versions and are the minimum required to resolve this issue: -

- Sophos Anti-Virus for Windows 2000/XP/2003/Vista 7.6.0
- Sophos Anti-Virus for Windows 95/98/NT 4.7.16
- Sophos Anti-Virus for Mac OSX 4.9.15
- Sophos Anti-Virus for Linux 6.4.4

Sophos customers can contact the company's technical support for additional assistance if required.

1 Detailed Vulnerability Description

1.1 Introduction

The Sophos Remote Management System is software used by the remote management component of Sophos software including the Sophos Enterprise Console (SEC). Sophos describe the SEC product as follows: -

“Sophos Enterprise Console is a management console that can be used to install Sophos Anti-Virus and Sophos Client Firewall remotely, and to configure, monitor, manage and report on Sophos products running on Windows and Mac OS X computers.”

Source: <http://www.sophos.com/readmes/readec.txt>

The SEC software allows administrators to connect to a centralised Dashboard service which can be used to search for and manage instances of Sophos Anti-Virus.

1.2 Technical Background

The Sophos Enterprise Console is a networked management portal through which instances of Sophos Anti-Virus can be managed across an Enterprise environment. The Enterprise Console communicates with the individual instances of Sophos Anti-Virus using a CORBA service.

The Remote Management System in Sophos products opens the following TCP ports for connection: -

- Port 8192 provides information about the Common Object Request Broker Architecture (CORBA) enabled service using an Interoperable Object Reference (IOR). This instructs the client software which port to connect to for the service and includes other information such as the name of the service.
- Port 8193 is the CORBA endpoint which is used to communicate with the Enterprise Console itself. This port operates in clear text and is therefore potentially vulnerable to traffic sniffing attacks.
- Port 8194 is the SSL enabled version of the CORBA service on port 8193.

Information about the CORBA service can be recovered by connecting to port 8192. An example of the IOR string is shown below: -

```
IOR:010000002600000049444c3a536f70686f734d6573736167696e672f4d657373616765526f757465
723a312e3000000010000000000000a000000010102000b00000031302e302e302e31333100000120
00004100000014010f004e55500000002100000000010000000526f6f74504f4100526f75746572506572
73697374656e740003000000010000004d657373616765526f75746572000000030000000000000800
00000115e100004f415401000000140000000115e1000100010000000000901010000000001400000
080000000115a60086000220
```

This string can be decoded using a Unix command line tool (such as “catior”) to give information about the CORBA service as can be observed here: -

```
The Byte Order: Little Endian
The Type Id: "IDL:SophosMessaging/MessageRouter:1.0"
```

```

Number of Profiles in IOR:      1
Profile number: 1
IIOP Version: 1.2
  Host Name: 10.0.0.131
  Port Number: 8193
  Object Key len: 65
  Object Key as hex:
  14 01 0f 00 4e 55 50 00 00 00 21 00 00 00 00 01
  00 00 00 52 6f 6f 74 50 4f 41 00 52 6f 75 74 65
  72 50 65 72 73 69 73 74 65 6e 74 00 03 00 00 00
  01 00 00 00 4d 65 73 73 61 67 65 52 6f 75 74 65
  72
  The Object Key as string:
  ....NUP...!......RootPOA.RouterPersistent.....MessageRouter
  The component <1> ID is 0 (TAG_ORB_TYPE)
    ORB Type: 1413566208 (TAO)
  The component <2> ID is 1 (TAG_CODE_SETS)
    Component Length 20
    The Component Byte Order: Little Endian
    Native CodeSet for char: Hex - 10001 Description - ASCII
    Number of CCS for char 0
    Native CodeSet for wchar: Hex - 10109 Description - Unicode
    Number of CCS for wchar 0
  The component <3> ID is 20
    Component Value len: 8
    Component Value as hex:
    01 15 a6 00 86 00 02 20
    The Component Value as string:
    .....
cator returned true
  
```

The Enterprise Console service can be communicated with using the General Inter Orb Protocol (GIOP). This is used to communicate with a CORBA enabled service which is utilised by the Enterprise Console and endpoints. The CORBA interface within the Sophos software is provided by the ACE+TAO package.

The GIOP packet includes a “Message Length” field which has been highlighted in the screen shot below:

```

0000  00 0c 29 4e 54 4d 00 16 36 28 bc dd 08 00 45 00  ..)NTM.. 6(.E.
0010  00 90 09 1a 40 00 80 06 db 72 0a 0a 00 e5 0a 0a  ...@... .r.....
0020  00 e3 04 4d 20 01 31 5b fa af d1 11 16 9f 50 18  ...M .1[ .....P.
0030  ff ff 70 35 00 00 47 49 4f 50 01 02 01 00 5c 00  ..p5..GI OP....\
0040  00 00 0f 00 00 00 03 00 00 00 00 00 71 89 23 00  ..)..... .q.#.
0050  00 00 14 01 0f 00 4e 53 54 c9 95 e1 46 1c 4e 0e  .....NS T...F.N.
0060  00 01 00 00 00 01 00 00 00 03 00 00 00 01 00 00  .....
0070  00 04 00 00 00 72 0a 00 00 00 48 65 61 72 74 62  .....r.. ..Heartb
0080  65 61 74 00 65 00 01 00 00 00 01 00 00 00 0c 00  eat.e... .....
0090  00 00 01 e0 e3 00 01 00 01 00 09 01 01 00  .....
  
```

This field is used to indicate the length of the data which follows in the packet.

1.3 Vulnerability Details

A vulnerability was discovered such that an attacker could cause the Remote Management System router service to terminate if a packet was received with an invalid “Message Size” length field. For example, a value of 0x7FFFFFFF would trigger the vulnerability, if supplied in the first data packet of the communication with the service. A number of other values will also trigger this vulnerability but these are expected to be part of a limited range.

The invalid length field appears to be correctly detected and handled by the CORBA implementation and is then handed on to the Sophos code running the Enterprise Console. This software appears to detect the error condition and terminates the NTRouter.exe process and hence the “Sophos Message Router” service. When this process terminates no further connections to port 8193 (or port 8194) are accepted and therefore administrative tasks cannot be completed.

1.4 Vulnerability Impact

The successful exploitation of this vulnerability would prevent communications between the SEC and instances of Sophos Anti-Virus due to the unavailability of the router service. This could have an impact on the ability to manage Sophos endpoints although it will not prevent definitions from being updated or the level of protection.

1.5 Exploit Information

The easiest method of exploiting the vulnerability is to send the affected service a specially crafted CORBA packet with the invalid length field. If this packet is sent, the service will terminate as described in this document.

MWR InfoSecurity has been able to construct a working DoS attack for Microsoft Windows platforms and whilst the attack is trivial to perform the code will not be released into the public domain at the present. The decision to release such code in the future will be taken based on MWR InfoSecurity’s obligations to protect its customers and Critical National Infrastructure (CNI) whilst also enabling the security community to accurately assess the vulnerability of systems running the software.

1.6 Dependencies

The ability of the Sophos Enterprise Console to restart itself on Operating Systems with a Service Management facility is governed by a parameter within the service configuration. By default this value is set to 1 minute meaning that the service should restart after 60 seconds. If an attacker were to send a packet to the service every 1 minute this would constitute an effective DoS condition. Setting this value to 0 minutes would minimise the risk from this vulnerability although constantly restarting the service might cause other issues. One such issue relates to the exploitation of vulnerabilities which require a service to be brute forced to find, for example, a valid return address. Such a setting will reduce the effectiveness of defensive techniques such as address space randomisation and therefore should be considered an interim solution only.

It should be noted that Operating Systems such as Windows 9x and some UNIX variants will not automatically restart the service and will require manual intervention.

2 Recommendations

It is recommended that all users should install the appropriate security patches released by the vendor in response to this issue.

The issue has been resolved in RMS 3.0.9 and above. The following versions and are the minimum that are required to resolve this issue: -

- Sophos Anti-Virus for Windows 2000/XP/2003/Vista 7.6.0
- Sophos Anti-Virus for Windows 95/98/NT 4.7.16
- Sophos Anti-Virus for Mac OSX 4.9.15
- Sophos Anti-Virus for Linux 6.4.4

Interim Workaround

One method for mitigating the risk associated with this issue is to use network filtering controls to protect the service, which runs on TCP port 8193 by default. This service is not required for Sophos Enterprise Console or endpoint communications although the SSL enabled service on TCP port 8194 is required.

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com