

[NEWS] Hi-Resolution System's MacAdministrator Hidden Files Disclosure and Access Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0049.html>

From: support@securiteam.com

Date: 10/19/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] Hi-Resolution System's MacAdministrator Hidden Files Disclosure and Access Vulnerability

Message-Id: <20011019144930.A1C1D138C9@mail.der-keiler.de>

Date: Fri, 19 Oct 2001 16:49:30 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Hi-Resolution System's MacAdministrator Hidden Files Disclosure and Access Vulnerability

SUMMARY

<MacAdministrator > MacAdministrator is a powerful management tool for computers running MacOS. It provides an extensive range of features, under administrator control, for large and small networks independent of server type.

DETAILS

Vulnerable systems:

MacAdministrator version 1.7

MacAdministrator version 2.0.4fc4

MacAdministrator allows using of the hidden file attribute on the HFS catalog system thus providing a way of maintaining and administrating a network of multiple users. It also provides the administrator with an override account on each node connected to MacAdministrator's virtual network. Further, MacAdministrator secures the Navigation services (the Standard File Manager APIs) in the MacOS development toolbox, from

Securiteam: [NEWS] Hi-Resolution System's MacAdministrator Hidd

accessing certain features (e.g. making sure hidden files do not show up and allowing access locking).

The problem comes in however, when certain programs are linked at compile time against the old version of the Macintosh toolkit or other custom crafted routines. This causes them to ignore the hidden file flags, which in turn leads to the disclosure of hidden files.

This in itself provides a problem, as users could venture into hidden folders and expose hidden filenames, possibly sensitive information that could compromise the privacy of other users or the system. Furthermore, users are also able to access and even open/read such unprotected hidden files on the system, increasing the likelihood of the user to view private information and sensitive system information.

Indeed this is what can be achieved with MacAdministrator's preference files, resident on every computer node in its virtual network (distribution design feature). The file would allow a malicious user the possibility to disclose settings and manipulate vital configurations settings of the MacAdministrator system (as files do not appear to be read-only), and even gain access to the override account name and encrypted password (which would effectively compromise all override accounts on the connected nodes if the user in turn compromised the password).

Part of the problem is that MacAdministrator relies on using hidden files to try securing a few sensitive/private files such as original extensions, control panels, preferences, and the user folders of other users (user folders are however also coupled with access locking preventing exposure of docs, but does give indication of what login names are available).

Exploit:

Proof of concept can be presented by compiling the example program "HexDump" (user account required) provided by the Think Pascal 4.0 program package and then using it to browse through the file system hierarchy. Because Think Pascal provides its own runtime library with custom routines and toolbox (released from some OLD MacOS release) it neglects to handle hidden files properly.

Suggested solution:

The long and strenuous solution is for Hi-Resolution Systems to make MacAdministrator secure system routines by restriction of some sort and mandatory locking of configuration files (administrators do not appear to be able to do so by configuration currently).

Current administrators are advised to tighten configurations a lot more by allowing a certain set of applications execution privileges only so rogue programs cannot be run which may pose a security risk and perhaps update older applications in favor of newer releases that have been compiled against a newer Mac Toolbox. Hiding files should also not be relied on for protecting sensitive information.

Securiteam: [NEWS] Hi-Resolution System's MacAdministrator Hidd

ADDITIONAL INFORMATION

The information has been provided by <mailto:mithrandir@geek.com> MD5.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- *Previous message:* support@securiteam.com: "[NEWS] CDP Vulnerability in Cisco Routers"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)