CSIS Advisory

File Expert "path" Parameter Directory Traversal Vulnerability

Document written and evaluated by:
Sarid Harper
sha@csis.dk

Technical report

Publish date: juli 16, 2011

Contents

1 Summary

Sarid Harper has discovered a vulnerability in File Expert for Android, which can be exploited by malicious users to gain knowledge of sensitive information.

Input passed to the "path" parameter in "/webapps/file/listing" is not properly sanitised before being used to display files and directories. This can be exploited to list arbitrary directories and files via directory traversal attacks.

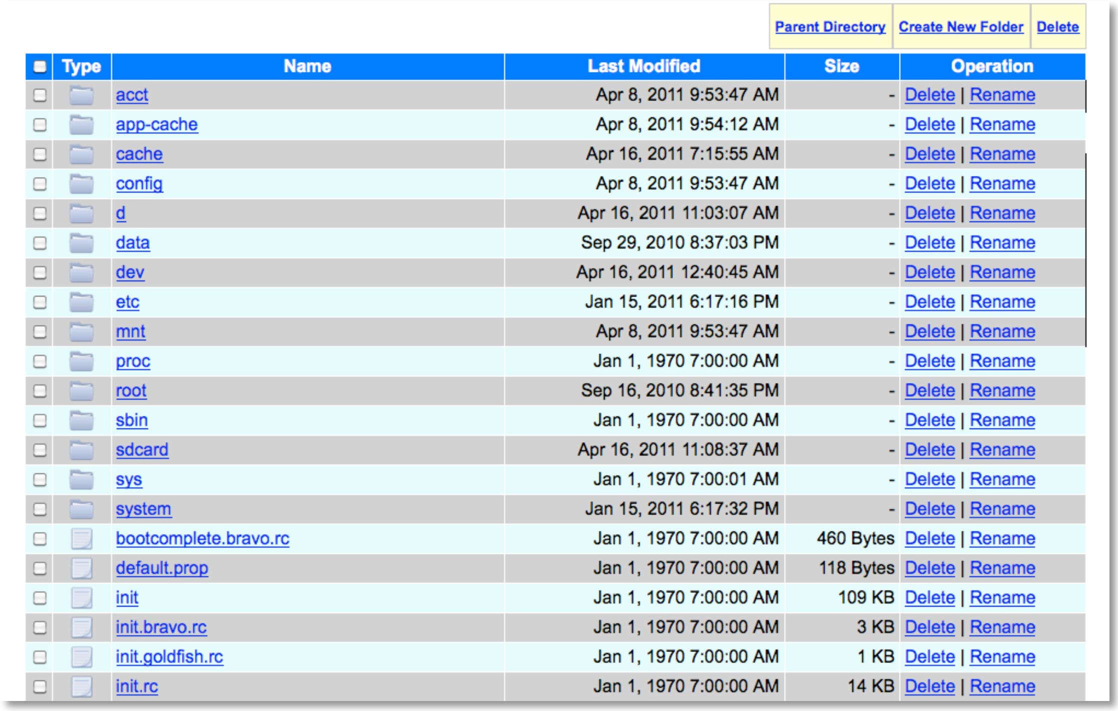
2 Affected Versions

This vulnerability is confirmed in the following version:

- The vulnerability is confirmed in version 3.1.2.

Other versions may also be affected.

3 Screen-dumps



■	Type	Name	Last Modified	Size	Operation
□	📁	acct	Apr 8, 2011 9:53:47 AM	-	Delete | Rename
□	📁	app-cache	Apr 8, 2011 9:54:12 AM	-	Delete | Rename
□	📁	cache	Apr 16, 2011 7:15:55 AM	-	Delete | Rename
□	📁	config	Apr 8, 2011 9:53:47 AM	-	Delete | Rename
□	📁	d	Apr 16, 2011 11:03:07 AM	-	Delete | Rename
□	📁	data	Sep 29, 2010 8:37:03 PM	-	Delete | Rename
□	📁	dev	Apr 16, 2011 12:40:45 AM	-	Delete | Rename
□	📁	etc	Jan 15, 2011 6:17:16 PM	-	Delete | Rename
□	📁	mnt	Apr 8, 2011 9:53:47 AM	-	Delete | Rename
□	📁	proc	Jan 1, 1970 7:00:00 AM	-	Delete | Rename
□	📁	root	Sep 16, 2010 8:41:35 PM	-	Delete | Rename
□	📁	sbin	Jan 1, 1970 7:00:00 AM	-	Delete | Rename
□	📁	sdcard	Apr 16, 2011 11:08:37 AM	-	Delete | Rename
□	📁	sys	Jan 1, 1970 7:00:01 AM	-	Delete | Rename
□	📁	system	Jan 15, 2011 6:17:32 PM	-	Delete | Rename
□	📄	bootcomplete.bravo.rc	Jan 1, 1970 7:00:00 AM	460 Bytes	Delete | Rename
□	📄	default.prop	Jan 1, 1970 7:00:00 AM	118 Bytes	Delete | Rename
□	📄	init	Jan 1, 1970 7:00:00 AM	109 KB	Delete | Rename
□	📄	init.bravo.rc	Jan 1, 1970 7:00:00 AM	3 KB	Delete | Rename
□	📄	init.goldfish.rc	Jan 1, 1970 7:00:00 AM	1 KB	Delete | Rename
□	📄	init.rc	Jan 1, 1970 7:00:00 AM	14 KB	Delete | Rename

4 Resolution

Upgrade to the latest version and grant access to trusted users only.

5 Time-line

1. Vulnerability identified: 09.04.11
2. Vendor informed: 16.04.11
3. Vendor response: 17.04.11
4. Vendor fix: 16.07.11

6 Credits

Vulnerability identified by Sarid Harper of the CSIS Security Group.

7 References

Geek Soft:
http://www.xageek.com/en/

CSIS:
http://www.csis.dk/