CSIS Advisory

File Expert File Deletion Vulnerability

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

Technical report

Publish date: juli 18, 2011

Contents

1 Summary

Sarid Harper has discovered a vulnerability in File Expert for Android, which can be exploited by malicious users to delete file residing outside the FTP root.

The vulnerability is caused by an error in the way FTP "DELE" requests are handled. This can be exploited to escape the FTP root and delete arbitrary files on the affected system by using the "../" character sequence.

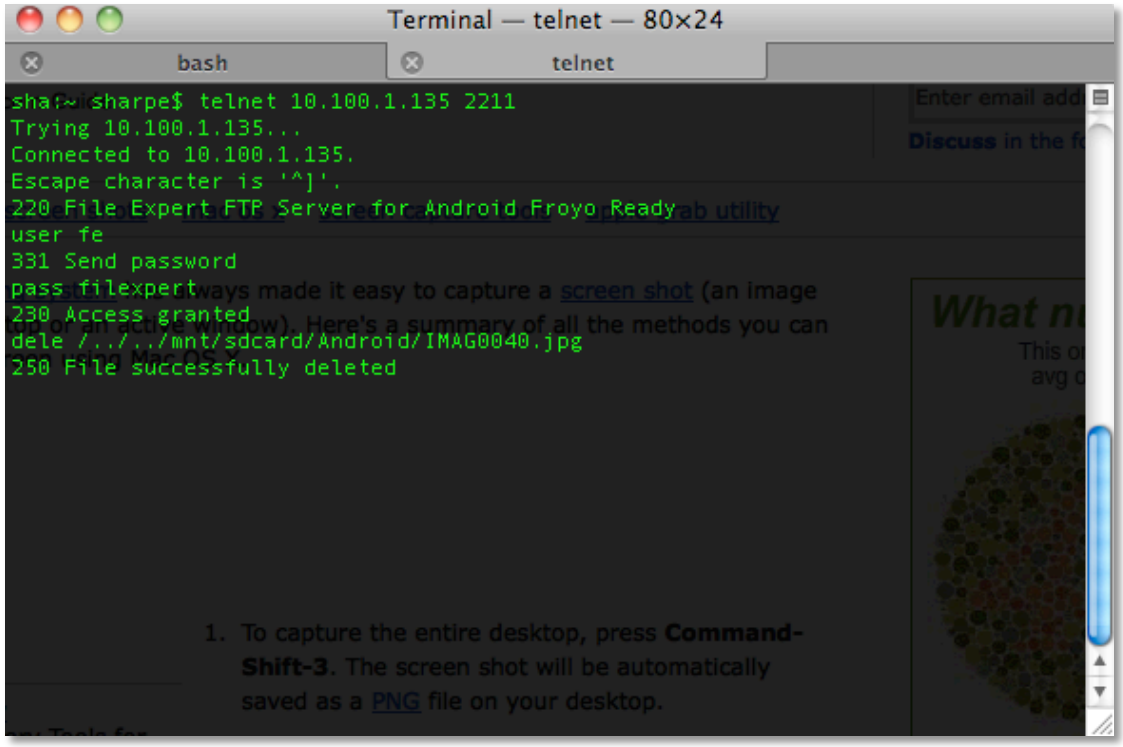
2 Affected Versions

This vulnerability is confirmed in the following version:

- The vulnerability is confirmed in version 3.0.4 and 3.0.5.

Other versions may also be affected.

3 Screen-dumps



4 Resolution

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

5 Time-line

1. Vulnerability identified: 19.04.11
2. Vendor informed: 19.04.11
3. Vendor response: 19.04.11
4. Vendor fix: 16.06.11

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/