



CVE-2012-5694

Published on: 10/20/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:20 PM UTC

CVE-2012-5694

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Smartphone Pentest Framework](#) from [Bulbsecurity](#) contain the following vulnerability:

Multiple SQL injection vulnerabilities in Bulb Security Smartphone Pentest Framework (SPF) before 0.1.3 allow remote attackers to execute arbitrary SQL commands via the (1) agentPhNo, (2) controlPhNo, (3) agentURLPath, (4) agentControlKey, or (5) platformDD1 parameter to frameworkgui/attach2Agents.pl; the (6)

modemPhoneNo, (7) controlKey, or (8) appURLPath parameter to frameworkgui/attachMobileModem.pl; the agentsDD parameter to (9) escalatePrivileges.pl, (10) getContacts.pl, (11) getDatabase.pl, (12) sendSMS.pl, or (13) takePic.pl in frameworkgui/; or the modemNoDD parameter to (14) escalatePrivileges.pl, (15) getContacts.pl, (16) getDatabase.pl, (17) SEAttack.pl, (18) sendSMS.pl, (19) takePic.pl, or (20) CSAttack.pl in frameworkgui/.

CVE-2012-5694 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

[osvdb.org](#)

[OSVDB 87324](#)

Inactive Link Not Archived

Security Advisory SA51414 - Smartphone
Pentest Framework frameworkgui Multiple

[web.archive.org](#)
[text/html](#)

[SECUNIA 51414](#)

Vulnerabilities - Secunia

No Description Provided

osvdb.org

OSVDB 87325

Inactive Link

Not Archived

Georgia Weidman on Twitter: "SPF GUI back in may god and infosec forgive me: https://t.co/uFeMXnmb"

Vendor Advisory

nitter.domain.glass

text/html

MISC

twitter.com/georgiaweidman/statuses/269138431567855618

File Not Found

Exploit

www.htbridge.com

text/html

Inactive Link

Not Archived

MISC

www.htbridge.com/advisory/HTB23123

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bulbsecurity	Smartphone Pentest Framework	0.1.2	All	All	All
Application	Bulbsecurity	Smartphone Pentest Framework	0.1.2	All	All	All

cpe:2.3:a:bulbsecurity:smartphone_pentest_framework:0.1.2:*:*:*:*:*:

cpe:2.3:a:bulbsecurity:smartphone_pentest_framework:0.1.2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →