



# CVE-2013-3689

Published on: 10/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

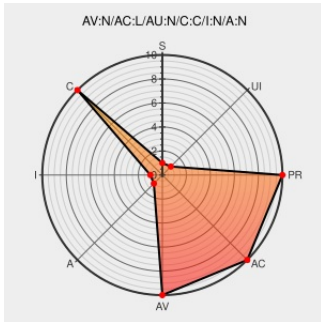
## CVE-2013-3689

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [100ap Device Firmware](#) from [Brickom](#) contain the following vulnerability:

Brickcom FB-100Ap, WCB-100Ap, MD-100Ap, WFB-100Ap, OB-100Ae, OSD-040E, and possibly other camera models with firmware 3.0.6.16C1 and earlier, do not properly restrict access to configfile.dump, which allow remote attackers to obtain sensitive information (user names, passwords, and configurations) via a get action.

CVE-2013-3689 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>COMPLETE</b>	<b>NONE</b>	<b>NONE</b>













## CVE References

Description	Tags	Link
Full Disclosure: Security Analysis of IP video surveillance cameras	<a href="#">seclists.org</a> <a href="#">text/html</a>	<a href="#">FULLDISC 20130612 Security Analysis of IP video surveillance cameras</a>

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](mailto: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
Operating System	Brickom	100ap Device Firmware	All	All	All	All
Hardware 	Brickom	Fb-100ap	-	All	All	All
Hardware 	Brickom	Fb-100ap	-	All	All	All
Hardware 	Brickom	Md-100ap	-	All	All	All
Hardware 	Brickom	Md-100ap	-	All	All	All
Hardware 	Brickom	Ob-100ae	-	All	All	All
Hardware 	Brickom	Ob-100ae	-	All	All	All
Hardware 	Brickom	Osd-040e	-	All	All	All
Hardware 	Brickom	Osd-040e	-	All	All	All
Hardware 	Brickom	Wcb-100ap	-	All	All	All
Hardware 	Brickom	Wcb-100ap	-	All	All	All
Hardware 	Brickom	Wfb-100ap	-	All	All	All
Hardware 	Brickom	Wfb-100ap	-	All	All	All
cpe:2.3:o:brickom:100ap_device_firmware:~::~::~:						
cpe:2.3:h:brickom:fb-100ap:~::~::~:						
cpe:2.3:h:brickom:fb-100ap:~::~::~:						
cpe:2.3:h:brickom:md-100ap:~::~::~:						
cpe:2.3:h:brickom:md-100ap:~::~::~:						
cpe:2.3:h:brickom:ob-100ae:~::~::~:						
cpe:2.3:h:brickom:ob-100ae:~::~::~:						
cpe:2.3:h:brickom:osd-040e:~::~::~:						
cpe:2.3:h:brickom:osd-040e:~::~::~:						
cpe:2.3:h:brickom:wcb-100ap:~::~::~:						
cpe:2.3:h:brickom:wcb-100ap:~::~::~:						
cpe:2.3:h:brickom:wfb-100ap:~::~::~:						
cpe:2.3:h:brickom:wfb-100ap:~::~::~:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**