

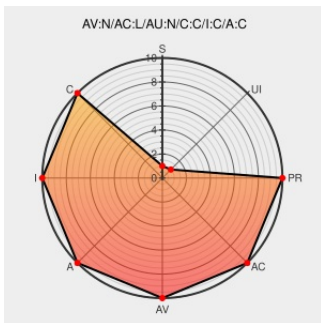


CVE-2013-6884

Published on: 01/07/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6884

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ditto Forensic Fieldstation](#) from [Cru-inc](#) contain the following vulnerability:

The write-blocker in CRU Ditto Forensic FieldStation with firmware before 2013Oct15a has a default "ditto" username and password, which allows remote attackers to gain privileges.

CVE-2013-6884 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Security Advisory SA55989 - Ditto Forensic FieldStation Multiple Vulnerabilities - Secunia

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

[SECUNIA 55989](#)

Ditto Firmware Release Notes 2013Jun30a | CRU

[Vendor Advisory](#)
[www.cru-inc.com](#)
[text/html](#)

[MISC www.cru-inc.com/support/software-downloads/ditto-firmware-updates/ditto-firmware-release-notes-2013jun30a/](#)

Full Disclosure: Ditto Forensic FieldStation, multiple vulnerabilities

[seclists.org](#)
[text/html](#)

[FULLDISC 20131212 Ditto Forensic FieldStation, multiple vulnerabilities](#)

Ditto Firmware Release Notes 2013Oct15a | CRU

[Vendor Advisory](#)
[www.cru-inc.com](#)
[text/html](#)

[MISC www.cru-inc.com/support/software-downloads/ditto-firmware-updates/ditto-firmware-release-notes-2013oct15a/](#)

Ditto Forensic FieldStation 2013Oct15a - Multiple Vulnerabilities

[Exploit](#)
[www.exploit-db.com](#)

[EXPLOIT-DB 30396](#)

Proof of Concept
text/html

Ditto Forensic FieldStation 2013Oct15a XSS/
CSRF / Command Execution ~ Packet Storm

Exploit
packetstormsecurity.com
text/html

MISC packetstormsecurity.com/files/124420/Ditto-
Forensic-FieldStation-2013Oct15a-XSS-CSRF-Command-
Execution.html

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
Hardware  	Cru-inc	Ditto Forensic Fieldstation	-	All	All	All
Hardware  	Cru-inc	Ditto Forensic Fieldstation	-	All	All	All
Operating System	Cru-inc	Ditto Forensic Fieldstation Firmware	All	All	All	All
cpe:2.3:h:cru-inc:ditto_forensic_fieldstation:-:*:*:*:*:*:						
cpe:2.3:h:cru-inc:ditto_forensic_fieldstation:-:*:*:*:*:*:						
cpe:2.3:o:cru-inc:ditto_forensic_fieldstation_firmware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© 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](#)