



CVE-2017-17105

Published on: 12/18/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:26 PM UTC

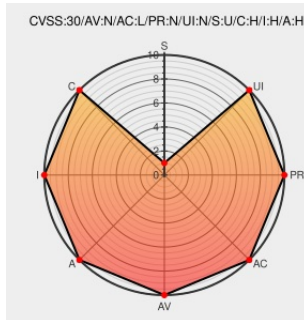
CVE-2017-17105

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Pr115-204-p-rs](#) from [Zivif](#) contain the following vulnerability:

Zivif PR115-204-P-RS V2.3.4.2103 and V4.7.4.2121 (and possibly in-between versions) web cameras are vulnerable to unauthenticated, blind remote command injection via CGI scripts used as part of the web interface, as demonstrated by a `cgi-bin/iptest.cgi?cmd=iptest.cgi&-time="1504225666237"&-url=$(reboot)` request.

CVE-2017-17105 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Zivif PR115-204-P-RS 2.3.4.2103 Bypass / Command Injection / Hardcoded Password ≈ Packet Storm	Exploit Third Party Advisory VDB Entry	MISC packetstormsecurity.com/files/145386/Zivif-PR115-204-P-RS-2.3.4.2103-Bypass-Command-Injection-Hardcoded-Password.html

[packetstormsecurity.com](#) [hardcoded-password.html](#)
[text/html](#)

Zivif Camera 2.3.4.2103 iptest.cgi Blind Remote Command Execution ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

 MISC
[packetstormsecurity.com/files/158120/Zivif-Camera-2.3.4.2103-ipctest.cgi-Blind-Remote-Command-Execution.html](#)

Full Disclosure: Three exploits for Zivif Web Cameras (may impact others)

[Exploit](#)
[Mailing List](#)
[Third Party Advisory](#)
[seclists.org](#)
[text/html](#)

 FULLDISC 20171212 Three exploits for Zivif Web Cameras (may impact others)

Silas Cutler na Twitterze: "Fun note. #LaCaja from @Hackerstrip is my disclosure for CVE-2017-17105, CVE-2017-17106, and CVE-2017-17107."

[Third Party Advisory](#)
[nitter.domain.glass](#)
[text/html](#)

 MISC
[twitter.com/silascutler/status/938052460328968192](#)

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 	Zivif	Pr115-204-p-rs	-	All	All	All
Hardware 	Zivif	Pr115-204-p-rs	-	All	All	All
Operating System	Zivif	Pr115-204-p-rs Firmware	2.3.4.2103	All	All	All
Operating System	Zivif	Pr115-204-p-rs Firmware	4.7.4.2121	All	All	All
Operating System	Zivif	Pr115-204-p-rs Firmware	2.3.4.2103	All	All	All
Operating System	Zivif	Pr115-204-p-rs Firmware	4.7.4.2121	All	All	All
cpe:2.3:h:zivif:pr115-204-p-rs:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:zivif:pr115-204-p-rs:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:zivif:pr115-204-p-rs_firmware:2.3.4.2103:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:zivif:pr115-204-p-rs_firmware:4.7.4.2121:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:zivif:pr115-204-p-rs_firmware:2.3.4.2103:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:zivif:pr115-204-p-rs_firmware:4.7.4.2121:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @MachinaRecord	このほか、 Zerobot 1.1が悪用するようになった新たな脆弱性には以下が含まれるそう： ・ CVE-2017-17105 (Zivif PR115-204-P-RS) ・ CVE-2019-10655 (Grandstream)... twitter.com/i/web/status/1...	2022-12-21 22:26:49
 @inthewildio	CVE-2022-45359 is getting exploited #inthewild. Find out more at inthewild.io/vuln/CVE-2022-... CVE-2017-17105 is getting... twitter.com/i/web/status/1...	2023-01-01 10:08:14

[← 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](#)