

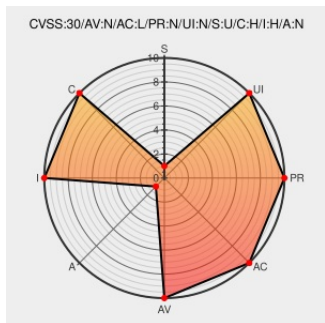


CVE-2017-9097

Published on: 06/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2017-9097

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

Certain versions of [Antiweb](#) from [Hoytech](#) contain the following vulnerability:

In Anti-Web through 3.8.7, as used on NetBiter FGW200 devices through 3.21.2, WS100 devices through 3.30.5, EC150 devices through 1.40.0, WS200 devices through 3.30.4, EC250 devices through 1.40.0, and other products, an LFI vulnerability allows a remote attacker to read or modify files through a path traversal

technique, as demonstrated by reading the password file, or using the template parameter to cgi-bin/write.cgi to write to an arbitrary file.

CVE-2017-9097 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Corbin, Alex	CVE-2017-9097	MISC: mitralabs: back:blognetal/2017/05/anna-industrial-at-over-cvss-cvss-anti

Capitan Alfa	Mailing List Third Party Advisory misteralfa-hack.blogspot.cl text/html Inactive Link Not Archived	MISC misteralfa-hack.blogspot.cl/2017/05/apps-industrial-ot-over-server-anti-web.html
	Patch Vendor Advisory www.netbiter.com application/zip	MISC www.netbiter.com/docs/default-source/netbiter-english/software/hms-security-advisory-2017-05-24-001-ws100-ws200-ec150-ec250.zip
Page not found - GitHub · GitHub	Third Party Advisory github.com text/html Inactive Link Not Archived	MISC github.com/ezelf/industrial_Tools/tree/master/scadas_server_antiweb/LFI

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

Exploit/POC from Github

Suite de herramientas que sacan partido del CVE-2017-9097 (+RCE)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hoytech	Antiweb	3.0.7	hms2	All	All
Application	Hoytech	Antiweb	3.3.5	All	All	All
Application	Hoytech	Antiweb	3.6.1	All	All	All
Application	Hoytech	Antiweb	3.7.1	All	All	All
Application	Hoytech	Antiweb	3.7.2	All	All	All
Application	Hoytech	Antiweb	3.8.1	All	All	All
Application	Hoytech	Antiweb	3.8.2	All	All	All
Application	Hoytech	Antiweb	3.8.3	All	All	All
Application	Hoytech	Antiweb	3.8.4	All	All	All
Application	Hoytech	Antiweb	3.8.5	All	All	All
Application	Hoytech	Antiweb	3.0.7	hms2	All	All
Application	Hoytech	Antiweb	3.3.5	All	All	All
Application	Hoytech	Antiweb	3.6.1	All	All	All
Application	Hoytech	Antiweb	3.7.1	All	All	All
Application	Hoytech	Antiweb	3.7.2	All	All	All
Application	Hoytech	Antiweb	3.8.1	All	All	All
Application	Hoytech	Antiweb	3.8.2	All	All	All

Application	Hoytech	Antiweb	3.8.2	All	All	All
Application	Hoytech	Antiweb	3.8.3	All	All	All
Application	Hoytech	Antiweb	3.8.4	All	All	All
Application	Hoytech	Antiweb	3.8.5	All	All	All
Application	Hoytech	Antiweb	All	All	All	All
cpe:2.3:a:hoytech:antiweb:3.0.7:hms2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.3.5:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.6.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.7.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.7.2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.3:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.4:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.5:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.0.7:hms2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.3.5:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.6.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.7.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.7.2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.1:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.2:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.3:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.4:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:3.8.5:~::~~::~~::						
cpe:2.3:a:hoytech:antiweb:~::~~::~~::						

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](#)