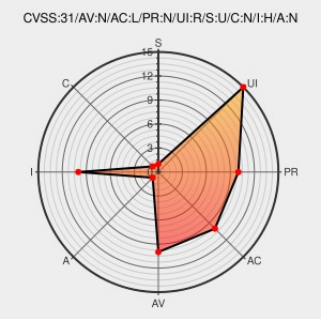
CVE-2020-25015

Published on: 09/16/2020 12:00:00 AM UTC

Last Modified on: 11/16/2022 02:14:00 PM UTC

CVE-2020-25015

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Platinum 4410 from Genexis contain the following vulnerability:

A specific router allows changing the Wi-Fi password remotely. Genexis Platinum 4410 V2-1.28, a compact router generally used at homes and offices was found to be vulnerable to Broken Access Control and CSRF which could be combined to remotely change the WIFI access point's password.

CVE-2020-25015 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Genexis Platinum 4410 Router - Broken Access Control, CSRF	Exploit Third Party Advisory web.archive.org	MISC www.getastra.com/blog/911/csrf-broken-access-control-in-genexis-platinum-4410/

	text/html Inactive Link Not Archived	
Genexis Platinum-4410 P4410-V2-1.28 Missing Access Control / CSRF ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159936/Genexis-Platinum-4410-P4410-V2-1.28-Missing-Access-Control-CSRF.html
Broken Access Control + CSRF in Genexis Platinum 4410 Router	Exploit Third Party Advisory www.jinsonvarghese.com text/html	MISC www.jinsonvarghese.com/broken-access-control-csrf-in-genexis-platinum-4410/

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	Genexis	Platinum 4410	2.1	All	All	All
Hardware	Genexis	Platinum 4410	2.1	All	All	All
Operating System	Genexis	Platinum 4410 Firmware	p4410-v2-1.28	All	All	All
Operating System	Genexis	Platinum 4410 Firmware	p4410-v2-1.28	All	All	All

cpe:2.3:h:genexis:platinum_4410:2.1:*:*:*:*:*:*:*:

cpe:2.3:h:genexis:platinum_4410:2.1:*:*:*:*:*:*:*:

cpe:2.3:o:genexis:platinum_4410_firmware:p4410-v2-1.28:*:*:*:*:*:*:*:

cpe:2.3:o:genexis:platinum_4410_firmware:p4410-v2-1.28:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← 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 registred 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