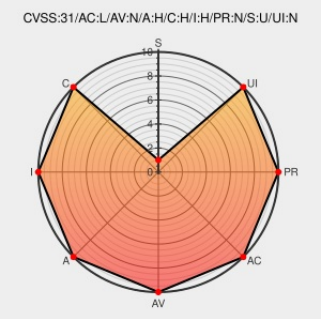
CVE-2022-33174

Published on: Not Yet Published

Last Modified on: 06/27/2022 04:45:00 PM UTC

CVE-2022-33174

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



Certain versions of Basic Pdu from Powertekpdus contain the following vulnerability:

Power Distribution Units running on Powertek firmware (multiple brands) before 3.30.30 allows remote authorization bypass in the web interface. To exploit the vulnerability, an attacker must send an HTTP packet to the data retrieval interface (/cgi/get_param.cgi) with the tmpToken cookie set to an empty string followed by a semicolon. This bypasses an active session authorization check. This can be then used to fetch the values of protected sys.passwd and sys.su.name fields that contain the username and password in cleartext.

CVE-2022-33174 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

Screams of Power vulnerabilities (Powertek-based PDUs) - gynvael.coldwind//vx.log	gynvael.coldwind.pl text/html	MISC gynvael.coldwind.pl/?lang=en&id=748

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Powertek PDU身份绕过

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Powertekpdus	Basic Pdu	-	All	All	All
Operating System	Powertekpdus	Basic Pdu Firmware	All	All	All	All
Hardware	Powertekpdus	Piml Pdu	-	All	All	All
Operating System	Powertekpdus	Piml Pdu Firmware	All	All	All	All
Hardware	Powertekpdus	Pm Pdu	-	All	All	All
Operating System	Powertekpdus	Pm Pdu Firmware	All	All	All	All
Hardware	Powertekpdus	Smart Pim	-	All	All	All
Operating System	Powertekpdus	Smart Pim Firmware	All	All	All	All
Hardware	Powertekpdus	Smart Pom	-	All	All	All
Hardware	Powertekpdus	Smart Poms	-	All	All	All
Operating System	Powertekpdus	Smart Poms Firmware	All	All	All	All
Operating System	Powertekpdus	Smart Pom Firmware	All	All	All	All
Hardware	Powertekpdus	Smart Pos	-	All	All	All
Operating System	Powertekpdus	Smart Pos Firmware	All	All	All	All

cpe:2.3:h:powertekpdus:basic_pdu:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:basic_pdu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:piml_pdu:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:piml_pdu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:pm_pdu:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:pm_pdu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:smart_pim:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:smart_pim_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:smart_pom:-:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:smart_poms:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:smart_poms_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:smart_pom_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:powertekpdus:smart_pos:-:*:*:*:*:*:*:*:

cpe:2.3:o:powertekpdus:smart_pos_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@gynvael	FTR CVE ids: CVE-2022-33174 CVE-2022-33175	2022-06-13 17:17:22
@CVEreport	CVE-2022-33174 : Power Distribution Units running on Powertek firmware multiple brands before 3.30.30 allows remo… twitter.com/i/web/status/1…	2022-06-13 18:06:40
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-33174 Power Distribution Units running on Powertek firmware (multiple b… twitter.com/i/web/status/1…	2022-06-13 18:56:01
@RedPacketSec	Powertek PDU Firmware information disclosure | CVE-2022-33174 - redpacketsecurity.com/powertek-pdu-f…	2022-06-14 09:01:24
@amirdaly0x00	Powertek PDUs 身份绕过等多个漏洞（CVE-2022-33174 CVE-2022-33175） dlvr.it/SS8fMm	2022-06-14 09:54:02
@hack_git	CVE-2022-33174 Powertek PDU Identity Bypass. github.com/Henry4E36/CVE-… #cve t.me/HackGit/5688 https://t.co/JMqs1tEvzs	2022-09-02 08:10:44
@Securityblog	GitHub - Henry4E36/CVE-2022-33174: Powertek PDU身份绕过 flip.it/_hfYUe	2022-09-03 11:24:33
@Prohacktiv3	? Surveillance des #POC (Proof Of Concept) sur @github : ? CVE-2022-33174: github.com/Henry4E36/CVE-… ? CVE-2021-3129… twitter.com/i/web/status/1…	2022-09-05 06:53:23
@OSINT_info	? Surveillance des #POC (Proof Of Concept) sur : ? CVE-2022-33174: github.com/Henry4E36/CVE-… ? CVE-2021-3129:… twitter.com/i/web/status/1…	2022-09-05 07:03:37
/r/netcve	CVE-2022-33174	2022-06-13 19:38:34

← Previous ID

Next ID→