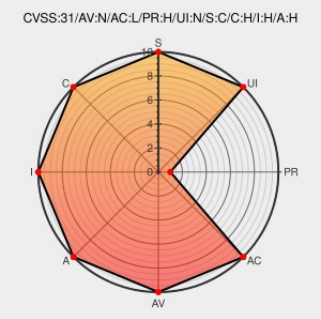
CVE-2022-29898

Published on: Not Yet Published

Last Modified on: 05/20/2022 02:16:00 PM UTC

CVE-2022-29898 - advisory for VDE-2022-018

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



Certain versions of Rad-ism-900-en-bd from Phoenixcontact contain the following vulnerability:

On various RAD-ISM-900-EN-* devices by PHOENIX CONTACT an admin user could use the configuration file uploader in the WebUI to execute arbitrary code with root privileges on the OS due to an improper validation of an integrity check value in all versions of the firmware.

CVE-2022-29898 has been assigned by info@cert.vde.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **PHOENIX CONTACT** - **RAD-ISM-900-EN-BD/B** version **= All Versions**

Affected Vendor/Software: **PHOENIX CONTACT** - **RAD-ISM-900-EN-BD** version **= All Versions**

Affected Vendor/Software: **PHOENIX CONTACT** - **RAD-ISM-900-EN-BD-BUS** version **= All Versions**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
VDE-2022-018 | CERT@VDE	cert.vde.com text/html	CONFIRM cert.vde.com/en/advisories/VDE-2022-018/

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.

Related QID Numbers

591316 Phoenix Contact RAD-ISM-900-EN-BD devices Multiple Vulnerabilities (VDE-2022-018)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Phoenixcontact	Rad-ism-900-en-bd	-	All	All	All
Hardware	Phoenixcontact	Rad-ism-900-en-bd-bus	-	All	All	All
Operating System	Phoenixcontact	Rad-ism-900-en-bd-bus Firmware	All	All	All	All
Hardware	Phoenixcontact	Rad-ism-900-en-bd/b	-	All	All	All
Operating System	Phoenixcontact	Rad-ism-900-en-bd/b Firmware	All	All	All	All
Operating System	Phoenixcontact	Rad-ism-900-en-bd Firmware	All	All	All	All

cpe:2.3:h:phoenixcontact:rad-ism-900-en-bd:-:*:*:*:*:*:*:*:

cpe:2.3:h:phoenixcontact:rad-ism-900-en-bd-bus:-:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:rad-ism-900-en-bd-bus_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:phoenixcontact:rad-ism-900-en-bd\/b:-:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:rad-ism-900-en-bd\/b_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:rad-ism-900-en-bd_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

The vulnerabilities were discovered and reported by Logan Carpenter of DRAGOS.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29898 : On various RAD-ISM-900-EN-* devices by PHOENIX CONTACT an admin user could use the configuration f… twitter.com/i/web/status/1…	2022-05-11 14:36:44
@LinInfoSec	Phoenix - CVE-2022-29898: cert.vde.com/en/advisories/…	2022-05-11

		17:06:55
@threatmeter	CVE-2022-29898 | Phoenix Contact RAD-ISM-900-EN WebUI improper validation of integrity check value (VDE-2022-018) A… twitter.com/i/web/status/1…	2022-05-12 07:08:55
/r/netcve	CVE-2022-29898	2022-05-11 15:39:19

← Previous ID

Next ID→