



CVE-2022-2640

Published on: Not Yet Published

Last Modified on: 12/06/2022 12:32:00 PM UTC

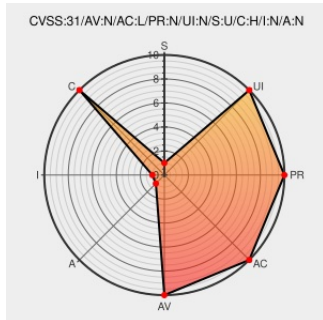
CVE-2022-2640

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Rcc972](#) from [Hornerautomation](#) contain the following vulnerability:

The Config-files of Horner Automation's RCC 972 with firmware version 15.40 are encrypted with weak XOR encryption vulnerable to reverse engineering. This could allow an attacker to obtain credentials to run services such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP).

CVE-2022-2640 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Horner Automation](#) - Remote Compact Controller (RCC) 972 version = 15.40

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

CVE References

Description	Tags	Link
Horner Automation Remote Compact Controller CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-22-335-02

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

[591343](#) Horner Automation Remote Compact Controller Inadequate Encryption Strength. Use of Hard-coded Cryptographic Key. Excessive

Horner Automation Remote Compact Controller Inadequate Encryption Strength, Poor Hard-coded Cryptographic Key, Excessive Reliance on Global Variables Multiple Vulnerabilities (ICSA-22-335-02)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Hornerautomation	Rcc972	-	All	All	All
Operating System	Hornerautomation	Rcc972 Firmware	15.40	All	All	All
cpe:2.3:h:hornerautomation:rcc972:-:*:*:*:*:*:						
cpe:2.3:o:hornerautomation:rcc972_firmware:15.40:*:*:*:*:*:						

Discovery Credit

m1etz reported these vulnerabilities through the Computer Emergency Response Team, CERT-Bund, to CISA

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2640 : The Config-files of Horner Automation's RCC 972 with firmware version 15.40 are encrypted with weak... twitter.com/i/web/status/1...	2022-12-02 20:09:42
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2022-2640 ift.tt/3wbogAe	2022-12-02 21:15:47
 @xanadulinux	CVE-2022-2640 ift.tt/6pTwM24	2022-12-02 21:16:43
 @doogsineerg	New vulnerability on the NVD: CVE-2022-2640 ift.tt/Xfug64p	2022-12-02 21:49:20
 @workentin	New vulnerability on the NVD: CVE-2022-2640 ift.tt/qUfSXAj	2022-12-02 21:54:39
 /r/netcve	CVE-2022-2640	2022-12-02 21:03:44

[← 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](#)