Honeywell

SECURITY NOTIFICATION SN 2021-02-22 01

SNs are Proprietary to Honeywell HPS and Honeywell HPS Customers

SNs describe a product security issue that is of an immediate nature which requires customer evaluation and potential action.

This SN is available on the Honeywell Online Support Web Site, at https://www.honeywellprocess.com/.

AFFECTED PRODUCT: **EXPERION PKS C200, C200E, C300 and ACE Controllers**
RELEASE/VERSION/REVISION: **All Experion PKS releases**
RELEASE DATE: **February 22th, 2021**
PAR: **1-CRQWQUD**

AFFECTED CUSTOMERS:

All Experion PKS customers using a C200, C200E, C300 or ACE controller, whether using CCLs or not.

VULNERABILITY OVERVIEW:

A Control Component Library (CCL) may be modified by a bad actor and loaded to a controller such that malicious code is executed by the controller.

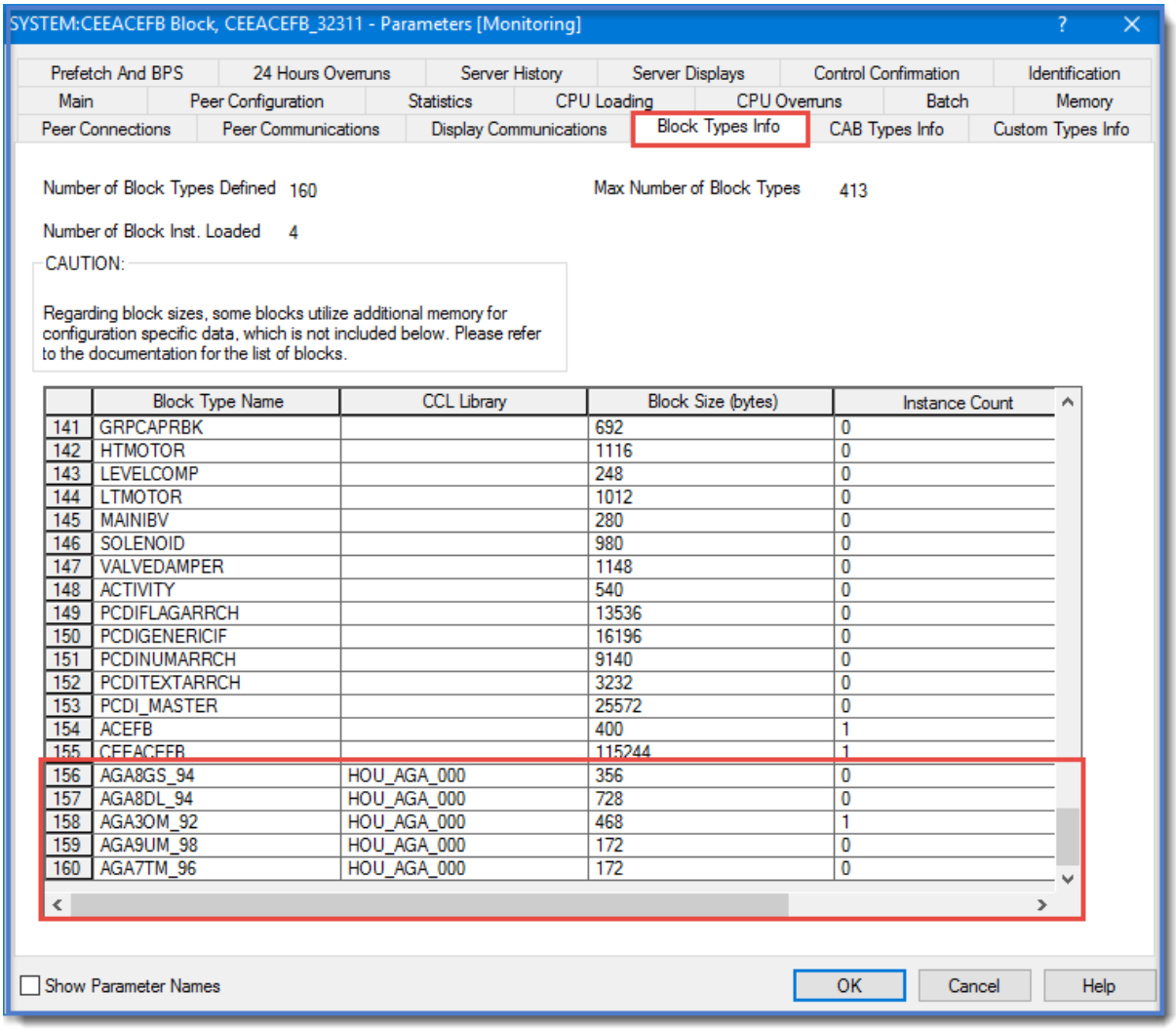
VULNERABILITY DETAILS:

A CCL is a library of control components that is loaded to a controller to perform specific functions. It is possible for a bad actor to modify a standard CCL to include malicious code, and to load the modified code to the controller and execute it.

Examples of standard CCLs are as follows (using the base names of the CCL files themselves):

- BLR_AGA10
- BRB_BOOLCTL
- BRB_CONVERT
- BRB_NORSOK
- BRB_SERVICE2
- BRB_VCONE
- BRB_WEGCTL
- FTW_ABDRIVEIF
- FTW_EXCHANGE
- FTW_FBUSIF
- FTW_HARTIO
- FTW_JAGXTREME
- FTW_PBUSIF
- FTW_PULSEIN
- FTW_QIMPACT
- FTW_RAILIO
- HON_API_NGL
- HON_TOOLKITB
- HOU_AGA
- PEK_API
- PEK_FISCALTOT
- PEK_ISO
- PHX_DNETIF
- PHX_FLEXIO

The vulnerability exists whether using these libraries or not, but this list is provided as a way to identify if a CCL is being used. This can be checked in the “Block Type Info” of the CEE Tab as shown in the example below.



	Block Type Name	CCL Library	Block Size (bytes)	Instance Count
141	GRPCAPRBK		692	0
142	HTMOTOR		1116	0
143	LEVELCOMP		248	0
144	LTMOTOR		1012	0
145	MAINIBV		280	0
146	SOLENOID		980	0
147	VALVEDAMPER		1148	0
148	ACTIVITY		540	0
149	PCDIFLAGARRCH		13536	0
150	PCDIGENERICIF		16196	0
151	PCDINUMARRCH		9140	0
152	PCDITEXTARRCH		3232	0
153	PCDI_MASTER		25572	0
154	ACEFB		400	1
155	CEEACEFB		115244	1
156	AGA8GS_94	HOU_AGA_000	356	0
157	AGA8DL_94	HOU_AGA_000	728	0
158	AGA3OM_92	HOU_AGA_000	468	1
159	AGA9UM_98	HOU_AGA_000	172	0
160	AGA7TM_96	HOU_AGA_000	172	0

CAUTION: Due to the wide variety of process control equipment configurations and site-specific control strategies, it is the responsibility of each customer to assess the potential impact of this anomaly to their process & facilities.

ACTIONS/MITIGATIONS:

A solution has been developed that uses cryptographic signing of CCLs. Although CCL binaries themselves are not modified, there is now an associated signature file for each CCL which is imported into the Experion PKS ERDB and sent to the controller when the CCL is loaded. This CCL signature file is validated before the CCL itself will be used.

A patch strategy has been developed for the controllers/impacted Experion PKS Versions. This patch includes both server software and controller firmware which are both needed to mitigate the issue. Therefore, after installing the patch onto the Experion PKS system, all controllers must be updated with the new firmware. The complete installation instructions are included in the SCN for the given release.
Users of other supported Experion releases, please follow the guidance provided below.

This remote code execution vulnerability impacts all Experion PKS releases. The table below provides information about the patch release scheduled dates.

Note: Any supported point release that is not listed in the table below will require the customer to migrate to the latest point release for a given major Experion release in order to get the benefits of the fix. For example, a customer at R501.4 would need to migrate to the R501.6 hotfix to get the fix.

Experion PKS Controllers & Tools Patches	Patch release date
R510.2 Hotfix10	Released
R501.6 (Hotfix planned)	2021
R511.5 (release planned)	2021
All other Experion releases	No plans for a Patch Release

Note: The patch is only for C300. ACE and C200 controllers are not planned to be patched.

An update to this notification will be made once the unreleased patches are made available.

Mitigation recommended until the release patch is completely installed:
The vulnerability could be exploited as a result of a compromised network (e.g. unauthorized node attached to the network), or the compromise of a Windows node on the network. Follow all recommendations in the Experion Network and Security Planning Guide to prevent attacks by malicious actors (https://www.honeywellprocess.com/library/support/Documents/Experion/Network-and-Security-Planning-Guide-EPDOC-XX75-en-511C.pdf)

Note: Users of custom CCLs should update their custom CCLs with the appropriate signature files. Custom CCLs are not included in the regular Experion PKS release media – they are created on an as-needed basis and are delivered to customers via a separate channel. Users who are not sure if they are using custom CCLs should use the ERDB Consistency Checker and check the output for reference(s) to custom CCLs. If there is any reference to custom CCL in the output of this checker, then they will need to be updated. Contact HPS Technical Support if custom CCLs are being used in order to get information on how to receive updated CCLs and corresponding update scripts.

Subscribe for Automated Email Alerts:
Honeywell advises all users to subscribe for alerts on HoneywellProcess.com to receive an email alert every time a new Notification or patch is posted. A tutorial is available ("Learn to Subscribe" link at the bottom right hand side of any page of HoneywellProcess.com) to help guide you through the subscription process and to tailor subscriptions to be appropriate to your system and needs. In addition you may also Subscribe to the GTAC Knowledge Sharing Mails which provide users on a regular basis with valuable tips & tricks, lessons learned and recommendations.

Further support required?
If you have any questions concerning this notification, please contact your local Honeywell office or the HPS Technical Support Center. Visit HoneywellProcess.Com and select "Contact Us" for country-specific Customer Contact Numbers. After you log on to HoneywellProcess.Com you may also Search our Knowledge Base or Submit a Support Request to request help.

Approved by the Field Action Committee & Issued by Global TAC