

**IMPORTANT – PLEASE READ****Controller Stop/Halt Security Vulnerability****Summary**

A security vulnerability has been identified in RX3i and RSTI-EP CPUs that if successfully exploited could cause the device to enter Stop/Halt Mode, causing the device to become unavailable.

The vulnerability has been assigned a CVSS v3 score of 7.5 and may be exploited remotely with network access to the CPU using the SRTP protocol.

Products Affected

Part Number	Affected Version
IC695CPE305 IC695CPE310	PACSystems RX3i CPE305/310 version 9.20 and prior
IC695CPE330	PACSystems RX3i CPE330 version 9.21 and prior
IC695CPE400	PACSystems RX3i CPE400 version 9.30 and prior
EPSCPE100	PACSystems RSTi-EP CPE100 version 9.30 and prior
IC695CPU320 IC695CRU320	PACSystems CPU320/CRU320 all versions
ICRXICTL000	PACSystems RXi all versions
IC695CPU315	PACSystems CPU315 all versions

Resolution

The resolution for this issue depends on the controller. A firmware update is available for active controllers. End-of-Life controllers have a recommended product upgrade path. Details are provided in the following section.

Action Recommended

GE recommends that customers update product firmware using the appropriate download links.

IC695CPE305 – https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE305-PACSystems-RX3i-CPU-DN

– **Upgrade Kit:** CPE305_FW9_40_41G1733-MS10-000-A17.zip

IC695CPE310 – https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE310-PACSystems-RX3i-CPU-DN

– **Upgrade Kit:** CPE310_FW9_40_41G1734-MS10-000-A17.zip

IC695CPE330 – https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE330-PACSystems-RX3i-CPU-DN

– **Upgrade Kit:** CPE330_FW9_40_41G2016-FW01-000-A11.zip

IC695CPE400 – https://digitalsupport.ge.com/communities/en_US/Download/IC695CPE400-PACSystems-RX3i-Rackless-CPU-with-Field-Agent

– **Upgrade Kit:** CPE400_FW9_40_41G2376-FW01-000-A3.zip

EPSCPE100 - https://digitalsupport.ge.com/communities/en_US/Download/EPSCPE100-RSTi-EP-CPU-Firmware

-- **Upgrade Kit:** 41G2393-MS10-000-A2.zip

Note: A customer support account is required to access firmware

CPU320/CRU320/CPU315 and RXi are end-of-life. GE recommends upgrade to the CPE330 for CPU320/CRU320/CPU315 applications and for Rxi controllers the recommended upgrade path is CPE400.

To minimize the risk of exposure to this and any other vulnerabilities, GE recommends a defense in depth approach to protecting critical process control equipment. Guidance on technology and best practices to secure GE controllers from Cyber-attack can be found in the published Secure Deployment Guides for each of the platforms located at:

https://digitalsupport.ge.com/communities/en_US/Documentation/PACSystems-RXi-RX3i-and-Rx7i-Controller-Secure-Deployment-Guide-GFK-2830

Part Number	Recommended Version
IC695CPE305 IC695CPE310	PACSystems RX3i CPE305/310 v9.4 or later
IC695CPE330	PACSystems RX3i CPE330 v9.4 or later
IC695CPE400	PACSystems RX3i CPE400 v9.4 or later
EPSCPE100	PACSystems RSTi-EP CPE100 v9.35 or later
IC695CPU320 IC695CRU320	Upgrade to CPE330
ICRXICTL000	Upgrade to CPE400
IC695CPU315	Upgrade to CPE330

Special Note

GE thanks Younes Dragoni of Nozomi Networks who initially reported the vulnerability and ICS-CERT who posted advisory ICSA-18-137-01 dated 17 May 2018 related to this issue (<https://ics-cert.us-cert.gov/advisories/ICSA-18-137-01>)

Distributors / Channel Partners

You must personally contact all customers who may have received these units to ensure that they receive a copy of this bulletin.

Contact Information

- Contact our Technical Support team with any technical questions.
- Contact our Customer Care team with any warranty or order questions.
- Detailed contact information is provided on the following page.
- Make sure you have your Customer Service Number (CSN) when calling us. If you don't have one, sign up here: https://ge-ip.force.com/communities/CC_SignupPassword
- Locate a Distributor or Channel Partner: <http://www.geautomation.com/products/sales>

Contact Information

Please contact your local Automation & Controls office or GE's Automation & Controls PLC Technical Support for further technical information concerning this bulletin. Distributors can contact Customer Care.

Submit a support case online at: https://ge-ip.force.com/communities/CC_CommercialViewCases?type=all

Technical Support (Americas)

Online: https://ge-ip.force.com/communities/CC_CommercialViewCases?type=all

Phone: 1-800-433-2682

780-420-2010 (if toll free 800 option is unavailable)

Primary language of support: English

Technical Support (Europe, Middle East, & Africa)

Online: https://ge-ip.force.com/communities/CC_CommercialViewCases?type=all

Phone: +800-1-433-2682 (Choose Language> Option 2> CSN>Option 2)

+352-26-722-780 (if toll free 800 option is unavailable or dialing from a mobile telephone)

Primary languages of support: English, French, German, Italian, Spanish

Technical Support (Asia)

Online: https://ge-ip.force.com/communities/CC_CommercialViewCases?type=all

Phone: +86-400-820-8208

+86-21-3217-4826 (India, Indonesia & Pakistan)

Primary language of support: Standard Mandarin

Customer Care (Americas)

Phone: (800) 433-2682 or 780-420-2010

Option 1 (Automation), Option 2 (Enter CSN)

... then Option 1 (Customer Care), Option 5 (Speak to Advocate)

Email: customercare.ip@ge.com

Primary language of support: English

Customer Care (Europe, Middle East, and Africa)

Phone: +800-1-433-2682

Choose Language> Option 2> CSN>Option 2

General Email: customercare.emea.ip@ge.com

Primary languages of support: English, French, German, Italian, Czech, Spanish

Customer Care (Asia)

Phone: +86-400-820-8208

Phone: +86 21-3217-4826 (for India, Indonesia and Pakistan)

Greater China: Customercare.cn.ip@ge.com

Rest of Asia: Customercare.apo.ip@ge.com