America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Omron Multiple Product Vulnerabilities

Last Revised: January 31, 2019 **Alert Code:** ICSA-15-274-01

OVERVIEW

Air Force Institute of Technology researcher Stephen Dunlap has identified vulnerabilities in Omron Corporation's CX-Programmer software, CJ2M series programmable logic controller (PLC), and CJ2H series PLC. Omron Corporation has produced new versions that mitigate these vulnerabilities.

One of the three vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Omron Corporation products are affected:

- CX-Programmer software, versions prior to Version 9.6,

- CJ2M Series PLC, versions prior to Version 2.1, and
- CJ2H Series PLC, versions prior to Version 1.5.

IMPACT

Successful exploitation of these vulnerabilities could result in the compromise of sensitive account information.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Omron Corporation is an international company headquartered in Kyoto, Japan.

The affected product, CX-Programmer, is part of the CX-One software suite, which is used to configure and program devices such as PLCs and HMIs. The CJ2M series device is a PLC primarily used for packaging and machine automation. The CJ2H series device is a PLC used for machine automation that requires image processing inspection of electrical components and high speed sorting on conveyors. According to Omron Corporation, these products are deployed across the Critical Manufacturing sector. Omron Corporation estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATIONCWE-319: Cleartext Transmission of Sensitive Information, http://cwe.mitre.org/data/definitions/319.html, web site last accessed October 1, 2015.

The password is transmitted in clear text to unlock the PLC for modification, which leaves the password vulnerable to packet sniffing.

CVE-2015-0987NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0987, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H, web site last accessed October 1, 2015.

STORING PASSWORDS IN A RECOVERABLE FORMATCWE-257: Storing Passwords in a Recoverable Format, http://cwe.mitre.org/data/definitions/257.html, web site last accessed October 1, 2015.

Passwords are stored in source code protected project files for CX-Programmer in a recoverable format.

CVE-2015-0988NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0988, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is

(AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H, web site last accessed October 1, 2015.

STORING PASSWORDS IN A RECOVERABLE FORMATCWE-257: Storing Passwords in a Recoverable Format, http://cwe.mitre.org/data/definitions/257.html, web site last accessed October 1, 2015.

Passwords are locally stored in an object file that is saved in a Compact Flash Card in a recoverable format.

CVE-2015-1015NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1015, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H, web site last accessed October 1, 2015.

VULNERABILITY DETAILS

EXPLOITABILITY

The clear text transmission of sensitive information vulnerability could be exploited remotely. The storage of passwords in recoverable format vulnerabilities is locally exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with low skill would be able to exploit these vulnerabilities.

MITIGATION

Omron Corporation has released a new version of the CX-Programmer software (Version 9.6) and new versions of the CJ2M series PLC (Version 2.1) and the CJ2H Series PLC (Version 1.5), which resolve the identified vulnerabilities. Omron Corporation recommends installing the new versions as soon as possible.

The CX-Programmer software, Version 9.6, is available by auto-update service or at the following URL:

https://industrial.omron.us/en/products/catalogue/automation_systems/software/programming/cx-one/default.html
<https://industrial.omron.us/en/products/catalogue/automation_systems/software/programming/cx-one/default.html>

The CJ2M series PLC, Version 2.1 and the CJ2H series PLC, Version 1.5 can be obtained by contacting Omron Corporation's Customer Care Team:

https://industrial.omron.us/en/services-and-support/customer-care
<https://industrial.omron.us/en/services-and-support/customer-care>.

Omron Corporation's security notice is available at the following URL:

http://www.fa.omron.co.jp/product/special/security_plc/index.html
<http://www.fa.omron.co.jp/product/special/security_plc/index.html>.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should consider the following:

- Limit physical and logical access to ICS environments by implementing defense-in-depth strategies.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices </ics/content/recommended-practices>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/ </ics/>).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Omron

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov