Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2022-0010

Malware targeting ICS/SCADA systems

Original Issue Date: April 16, 2022

Severity Rating: Critical

Overview

It has been reported that advanced persistent threat (APT) actors are targeting Industrial Control Systems (ICS)/SCADA devices through custom made tools. The tools enable cyber threat actors to scan for, compromise and control affected devices after gaining initial access to the operational technology (OT) network. The threat actors can also elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions after compromising ICS/SCADA devices.

Description

The APT actors are targeting ICS/SCADA systems using custom made tools. The threat actors have capability to gain full system control of certain ICS/SCADA devices including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The cyber threat actors could also exploit a known-vulnerable ASRock-signed motherboard driver, AsrDrv103.sys, exploiting CVE-2020-15368 to execute malicious code in the Windows kernel to move laterally within an IT or OT environment and disrupt critical devices or functions.

Schneider Electric Devices

The APT actors' tool has modules that may allow cyber actors to conduct a rapid scan to identify all Schneider PLCs on the local network via UDP multicast with a destination port of 27127, allow to perform brute-force, conduct a DoS attack to prevent network communications, capture of credentials, conduct a ¿packet of death¿ attack, or may send custom Modbus commands.

OMRON devices

The APT actors' tool has modules that may allow to scan for OMRON devices using FINS protocol, parsing HTTP response, retrieving MAC address, conduct polling for specific devices connected to the PLC, backing up/restoring arbitrary files to/from the PLC, and Loading a custom malicious agent on OMRON PLCs for additional attacker-directed capability.

OPC UA devices

The APT actors' tool modules has functionality to identify OPC UA servers, creating connection with OPC UA server using default or previously compromised credentials, reading OPC UA structure, and potentially writing tag values available via OPC UA.

Best Practices

- Employ two-factor or multi-factor authorization (MFA/2FA) for remote access wherever possible.
- Deploy logical or physical means of network segmentation to separate IT and OT network of ICS/SACDA system using strong perimeter control.
- Ensure devices are properly configured, only application necessary for operation is installed, and corresponding security features is enabled.
- Apply software Restriction policies appropriately. Deploy least user privileges.
- Enforce a strong password policy and implement regular password changes for SCADA/ICS systems. The strong passwords would enable to prevent brute force attempts of attacks.
- Implement appropriate logging mechanism to store and analyse the log of perimeter and critical devices of ICS/SCADA systems and IT networks.
- Limit ICS/SCADA systems' network connections to only specifically allowed management and engineering workstations.
- Robustly protect management systems by configuring Device Guard, Credential Guard, and Hypervisor Code Integrity (HVCI). Install Endpoint Detection and Response (EDR) solutions on these subnets and ensure strong anti-virus file reputation settings are configured.
- Deploy the continuous OT monitoring solution to alert on malicious indicators and behaviours, watching internal systems and communications for known hostile actions and lateral movement.
- Create and maintain regular backups of files. The system may be recovered from backup in case of disruptive attacks. Note that backups be maintained offline as APT actors may attempt to find and delete any accessible backups.
- Use the best practices of preventing phishing, and malware propagation attacks.
- Use the best practices considering risk management and cyber hygiene practices of third parties or managed service providers.
- Use and exercise the incident response plan.
- Investigate symptoms of a denial of service or connection severing, which exhibit as delays in communications processing, loss of function requiring a reboot, and delayed actions to operator comments as signs of potential malicious activity.
- Monitor systems for loading of unusual drivers, especially for ASRock driver if no ASRock driver is normally used on the system.
- Secure the perimeter devices such as firewall, router, and critical servers. Implement strong password, and access control over them. Keep it up-to-date with patches and fixes application software to the latest version.

References

https://securityaffairs.co/wordpress/130195/apt/us-gov-warns-apt-targets-ics-scada.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
https://portswigger.net/daily-swig/critical-infrastructure-entities-on-red-alert-over-exceptionally-rare-and-dangerous-ics-malware

CVE Name
CVE-2020-15368

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India