Severity

High

Analysis Summary

APT groups have created custom-made tools to attack and infiltrate ICS/SCADA devices. These tools have been recently observed in control specific devices and attacks. The tools can be used to scan for affected devices, compromise them, and also control them. Known vulnerabilities are also being exploited by the threat actors. The following devices are being exploited by APT actors:

1. Schneider Electric MODICON and MODICON Nano PLCs, including (but may not be limited to) TM251, TM241, M258, M238, LMC058, and LMC078;
2. OMRON Sysmac NJ and NX PLCs, including (but may not be limited to) NEX NX1P2, NXSL3300, NX-ECC203, NJ501-1300, S8VK, and R88D-1SN10F-ECT; and
3. OPC Unified Architecture (OPC UA) servers.

A known vulnerability CVE-2020-15368 in which an ASRocksigned motherboard driver, AsrDrv103.sys is being exploited to run malicious codes on windows servers. Lateral movement and disruption of critical devices are only part of the attack capabilities of these APT tools. The tools can also:

1. Identify all Schneider PLCs by running a rapid scan.
2. Passwords for e Schneider Electric PLCs can also be identified using brute-force attacks.
3. Conduct a denial-of-service attack.
4. Crash PLCs using a “packet of death” attack.
5. Retrieve MAC addresses.
6. Backup and restore files from the PLC.

Impact

- Data Theft
- Denial Of Service
- System Performance Degradation
- Financial Loss

Affected Vendors

- Schneider Electric
- Omron
- OPC UA

Remediation

- ICS/SCADA systems and networks should be isolated from internal and corporate networks.
- Multifactor authentication should be enabled for all ICS networks.
- Have a cyber incident response plan, and exercise it regularly with stakeholders in IT, cybersecurity, and operations.
- Never maintain default passwords. Use unique and strong passwords to mitigate dictionary and brute-force attacks.
- Backup your data. Any damage in case of a successful attack will be mitigated if data is backed up.
- Limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- Set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Log your IT/OT environment’s network activity and web server activity.
- Monitor systems for loading of unusual drivers, especially for ASRock drivers.