TOP 10

CRITICAL INFRASTRUCTURE AND SCADA/ICS CYBERSECURITY VULNERABILITIES AND THREATS

Operational Technology (OT) Systems Lack Basic Security Controls. Below Are the Most Common Threats:

Vulnerabilities

01 > Legacy Software

OT Systems run on legacy software that lack sufficient user and system authentication, data authenticity verification, or data integrity checking features that allow attackers uncontrolled access to systems.

02 > Default Configuration

Out-of-box systems with default or simple passwords and baseline configurations make it easy for attackers to enumerate and compromise OT systems.

03 > Lack of Encryption

Legacy SCADA controllers and industrial protocols lack the ability to encrypt communication. Attackers use sniffing software to discover username and passwords.

04 > Remote Access Policies

SCADA systems connected to unaudited dial-up lines or remote-access servers give attackers convenient backdoor access to the OT network as well as the corporate LAN.

05 > Policies and Procedures

Security gaps are created when IT and OT personnel differ in their approach to securing industrial controls. Different sides should work together to create a unified security policy that protects both IT and OT technology.

Threats

06 > Lack of Network Segmentation

Internet connected OT flat and misconfigured network, firewall features that fail to detect or block malicious activity provide attackers a means to access OT systems.

07 > DDoS Attacks

Invalidated sources and limited access-controls allow attackers intent on sabotaging OT systems to execute DoS attacks on vulnerable unpatched systems.

08 > Web Application Attacks

Traditional OT systems including human-management interfaces (HMI) and programmable logic computers (PLC) are increasingly connected to the network and accessible anywhere via the web-interface. Unprotected systems are vulnerable to cross-site scripting and SQL injection attacks.

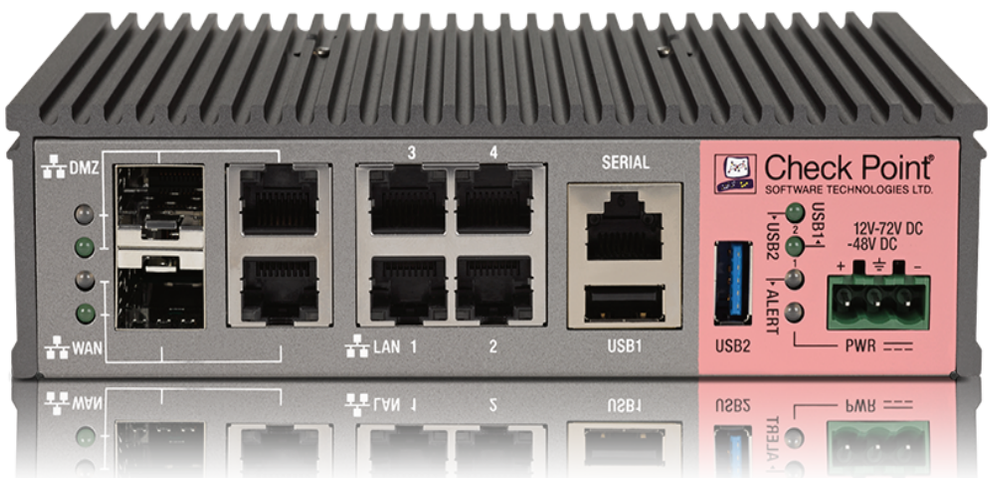
09 > Malware

OT Systems are vulnerable to attack and should incorporate anti-malware protection, host-based firewall controls, and patch-management policies to reduce exposure.

10 > Command Injection and Parameters Manipulation

Invalidated data not verified as legitimate system traffic allows attackers to execute arbitrary system commands on OT systems.

Industrial Control Systems (ICS) used in critical infrastructure and manufacturing industries are targets of sophisticated cyberattacks. The Check Point 1200R rugged appliance line delivers proven, integrated security for deployment in harsh environments as part of a complete end-to-end ICS security solution.



Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

To learn more about Check Point's Solutions for Critical Infrastructure, please visit www.checkpoint.com/ics

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2016 Check Point Software Technologies Ltd. All rights reserved.
March 2016