Power and Water Cybersecurity Suite – Vulnerability Assessment

Features

- Discovers network assets
- Assesses vulnerabilities and configurations
- Identifies risk
- Prioritizes threats
- Reports against compliance policies
- Ensures proactive risk management
- Delivers complete visibility of all assets
- Provides actionable information for orderly remediation
- One solution for complex environments

Overview

Software vulnerabilities are unintentional computer program weaknesses used by malicious actors to gain unauthorized access or privileges to a control system. Software patches are constantly developed and deployed to address these vulnerabilities; however, cyber-attacks can still be successful, especially on unpatched systems or applications. Notification of any unaddressed vulnerability is essential.

In conjunction with known threats, software vulnerabilities present different levels of risk to a control system and its operation. The metrics of properly assessed risks helps prioritize risk-mitigating tasks. A necessary best practice is to scan the control system for asset discovery and expose the known vulnerabilities. It is equally important to properly plan and execute the scanning task to avoid inadvertent threats to a stable operating environment, such as overwhelming the network's bandwidth with scanning activity.

A practical and prudent plan provides a balanced approach for accurately fingerprinting the control system and maintaining mission-critical performance.

Solution

Vulnerability Assessment is a Power and Water Cybersecurity Suite application that closes the gaps between vulnerabilities and risks through a reliable and flexible scanning tool.

Vulnerability management of a control system consists of proactively scanning the system's environment for vulnerabilities and providing guidance for mitigating risks.

The goals of vulnerability management include:

- Recognizing the security risks of the control environment including networks, operating systems, and other critical cyber assets.
- Exposing security threats including vulnerabilities and malware, as well as periodically updating threat intelligence.
- Ticketing discovered vulnerabilities.

Network-based or agentless scanning performs a comprehensive external examination of devices connected to the network. These devices include servers, desktop computers, laptops, routers, switches, printers, and any other unregistered devices.

Scan results are categorized as vulnerable, not vulnerable, or indeterminate data. The results are presented on a dashboard or within vulnerability assessment reports. The dashboard provides summary information for vulnerabilities, operating systems, severity, and vulnerability count trending. The vulnerability report is a compilation of information regarding the number of vulnerabilities found on the active systems scanned. These vulnerabilities can be viewed by severity (risk level), individual IP address, or operating system. Customized reports are available with the Vulnerability Assessment application.

Notification of scan-related events and remediation can be sent to pertinent personnel by Simple Network Management Protocol (SNMP) or email. Tickets created for vulnerabilities discovered during a scan can be used to help manage the process of remediating vulnerabilities.

Operations

The Vulnerability Assessment application is accessible through the Power and Water Cybersecurity Suite user interface browser. Access is protected by user identification and authentication. Multiple user roles are available and suitable for large deployments when several users are involved in the vulnerabilities discovery and remediation process.

Key operations in performing the assessment include:

- **Scans:** Performs asset discovery or vulnerability scans using standard or custom templates.
- **Components:** Groups assets by operating system, unit, or location. Multiple tags can be applied to an asset or multiple assets. Vulnerability sets can also be added for specific interest or importance. Vulnerability sets can be used in scan configurations, custom report templates, and asset tags.
- **Reports:** Views scan reports or generates custom reports.
- **Manage:** Sets risk score metrics, views current users and logs, manages data sources and assets, and sets notification and remediation rules.
- **Notification:** Enables the administrator to configure SNMP or email notification settings for remediation or scan-related events. Tickets can be created for vulnerabilities discovered during a scan. These tickets can be used to help manage the process of remediating vulnerabilities.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-010-4 R3 Parts 3.1, 3.2 and 3.3	Perform vulnerability assessment on cyber assets and provide documentation.	Generate vulnerability reports for compliance evidence.