PRODUCT DATA SHEET

Cardinal Technology Solutions, Inc.

Vulnerability Scanning & Remediation Service

NETWORK HARDENING INSIDE & OUT

Cyber Resilience & Identifying Vulnerabilities Early

Cyber resilience is the ability of an organization to sustain its business operations and processes despite adverse cyber circumstances. These can be in the form of cyber attacks, but can also be unintentional issues such as failed software updates or human error. Cyber resiliency goes beyond IT security. It's important to surface vulnerabilities early, prioritize them, and remediate them before they can be exploited by a cyber attack.

Looking At Infrastructure from an Attacker's Point of View: Using our Vulnerability Scanning Solution we can scan your external defenses (firewall) and also every aspect of your network from the inside as well. Every endpoint vulnerability is identified from workstations to switches, servers and firewalls. Vulnerabilities are identified using a database of over 100,000 published vulnerabilities and security policies. The database is updated on a regular basis so that the newest security information is available with each new scan.

Laser Focused Action: CTS engineers will first identify and then classify vulnerabilities. The next step is to prioritize which vulnerabilities need to be addressed first based on the information that comes back from the scans. The scans will identify weaknesses in data, applications, hosts and operating systems, network layers and perimeter defenses. Remedial actions are then taken against the issues that are surfaced, ensuring that potential attackers cannot exploit those weaknesses. The end objective is to completely harden your infrastructure by removing all known exploitable weaknesses.

Regularly Scheduled Scanning: Combined with our regular patching, monitoring, and maintenance of your network this service keeps you one step ahead of cyber criminals. It can be scheduled to run daily, monthly, or quarterly against the updated vulnerability database so you maintain your cyber resiliency.

Full Detailed Reporting: Scans are visible in the dashboard interface giving our engineers a birds-eye view of any issues that need to be addressed. We can see an overall picture of your security status using pie and bar charts that are color coded and prioritized on a threat level basis. We can also drill down into each identified issue for further analysis, see the details and take remedial action to close that vulnerability. Printable reports are available as well in PDF format. We can share the results of the scan and subsequent scans after actions are taken to show progress and current status.

Network Hardening: Scan for 100,000+ known vulnerabilities from the outside in, and from the inside out. Harden your defenses internally and externally.

Scan Automation: Scans can be scheduled on a custom basis for quarterly, monthly, weekly, or daily reports.

Updated Security Feeds: Once in place our solution checks daily for new updated vulnerability data.

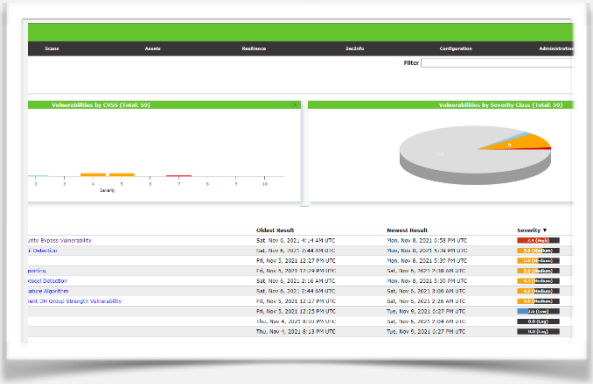
PREVENTION, DETECTION AND RESPONSE

Graphical Scan Summaries

This gives us the “birds-eye view” of the scan results, prioritizes actions based on threat level, and shows us an overall view of your current network security posture. After remedial action is taken, subsequent scans show progress made and next steps in the process by priority. Blue is good, orange is medium priority, red is critical priority.

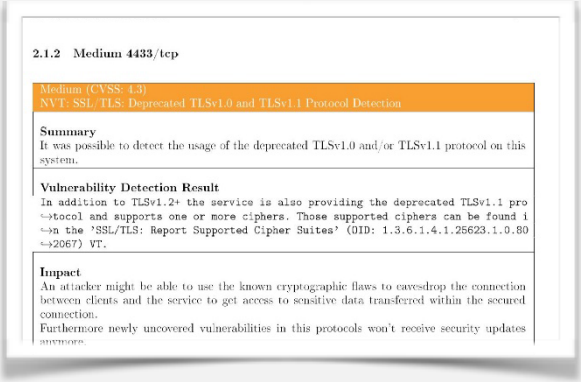
Detailed Visualization with Drilldown

We can visually render a complete list of vulnerabilities identified on your systems in detail, all prioritized by criticality. We can then drill down into each issue, see the specifics of what was identified as a threat and then take remedial action to remove the vulnerability.



Detailed Reporting

Once a scan is complete, we can share with you a detailed report of what the scan found. We can then discuss what the next steps should be. You will be able to see exactly what was identified, where it is on your network, the criticality of the vulnerability, and the action needed to harden the network.



2.1.2 Medium 4433/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.1 pro
↪tocol and supports one or more ciphers. Those supported ciphers can be found i
↪n the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.80
↪2067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Continued Proactive Scanning

As new machines and equipment are introduced into the environment and new vulnerabilities are identified over time, regular scheduled scans can keep your security posture strong. Your network will remain hardened, and you will be in the best possible defensive position.