

CUSTOMER ACTION REQUIRED:	YES <input type="checkbox"/>
	No <input checked="" type="checkbox"/>

NUMBER: 08-ISO-02
ISSUED BY: DEPUTY CIO, IT CUSTOMER DEVELOPMENT AND RELATIONSHIP MANAGEMENT SERVICES

CUSTOMER BULLETIN—(SECURITY AND RISK MANAGEMENT OFFICE)

TITLE: CIO/OFT VULNERABILITY TESTING PROGRAM
DATE ISSUED: August 12, 2008

Overview

The Office for Technology (CIO/OFT) has a robust vulnerability testing program that strives for excellence in maintaining the security of its computing environment and customer servers. CIO/OFT hosts over 2200 servers that contain data from over 25 state agencies.

CIO/OFT protects customer assets by regularly conducting vulnerability scans on the network infrastructure, servers, and key services. Vulnerability scanning is a process whereby dedicated security appliances probe networks, systems, and applications for insecure configurations and vulnerabilities in an effort to identify and correct those vulnerabilities before they are maliciously exploited.

Services Impacted: None

Audience

Agency Chief Information Officers (CIOs) and Information Security Officers (ISOs)

Assistance

If you have any questions or concerns related to the Vulnerability Testing program, please contact CIO/OFT IT Customer Development and Relationship Management Services at customer.relations@oft.state.ny.us.

Customer Action Required: No

Details

New vulnerabilities and exploits are constantly being identified. Consequently, CIO/OFT conducts monthly scans, both internally and externally. Internal scans check networks, systems, and devices for known vulnerabilities. An internal scan simulates what an "inside" attacker might find to potentially exploit a network or system. The scanning

device probes the target from within the network perimeter to identify weaknesses. External scans check networks, systems, and devices for known vulnerabilities using an Internet DSL account, which is completely separate from CIO/OFT's infrastructure. These systems and network devices are protected by firewalls and other network defenses. The scans simulate what an "outside" attacker might find to potentially exploit a network or system. The scanning device probes the target from outside the network perimeter to identify weaknesses.

CIO/OFT currently uses the McAfee Foundstone Enterprise 6.5 scanning solution, utilizing dedicated scanning appliances. This system uses a ranking system that compares the scanned environment against best practices to quantify the security risk. "High" and "medium" vulnerabilities present the greatest risk to the computing environment and is where CIO/OFT concentrates its remediation efforts. Because of the constant discovery of new exploits, it is impossible to eliminate all vulnerabilities. Rather, CIO/OFT focuses its efforts in keeping up with remediation in an attempt to minimize the risk that vulnerabilities present.

Vulnerability remediation is a labor-intensive activity that requires a high degree of human involvement to analyze data. Individuals with expertise in networking and operating system security are involved in the interpretation of the results. In cases where CIO/OFT hosts systems for other state entities, CIO/OFT is responsible for the remediation of vulnerabilities not specifically associated with the entity's application (e.g., operating system issues, hardware issues). If vulnerabilities associated with a state entity's application are found during a monthly scan, these results will be provided to the state entity's ISO via the NY-ISAC secure portal for their review and remediation.

Upon completion of vulnerability analysis, CIO/OFT takes the necessary actions to address the vulnerabilities found, including:

- Applying vendor patches
- Changing system configurations
- Adding external protections such as firewalls, ACLs, and Intrusion Prevention Systems

CIO/OFT must ensure that patches and other remedial actions are adequately tested prior to rolling them out into a production environment. Remediation, without testing, would negatively impact the availability of systems and applications. The remediation process includes the following procedures:

- Notifying change board prior to patching in "each" environment (development, QA, testing)
- Applying patches in each environment (development, QA, testing)
- Rolling out patches in a production environment (after the patches have passed the development, QA and testing processes).

The CIO/OFT vulnerability testing program is based on the National Institute of Standards and Technology (NIST) guidelines and controls, CSCIC's State Security Policy (P03-002 V3), and industry best practice.