Office of Inspector General

Computer Security Over Web Sites

Department of Transportation

Report Number: FI-2001-061
Date Issued: May 23, 2001

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **ACTION**: Report on Computer Security Over Web Sites, DOT FI-2001-061

Date: May 23, 2001

Reply To Attn Of:

From: Alexis M. Stefani
Assistant Inspector General for Auditing

To: Deputy Chief Information Officer

Because a web site of the Surface Transportation Board was hacked into on April 30, 2001, the Office of Inspector General (OIG) proactively examined computer security over Department of Transportation (DOT) web sites.

RESULTS

By using a commercial scanning software, we scanned 142 DOT web servers[1] and identified potential vulnerabilities on 86 servers in 8 DOT Operating Administrations. These potential vulnerabilities require detailed technical reviews to determine whether corrective actions are needed. Some vulnerabilities will require immediate corrective actions such as installing software fixes provided by computer manufacturers. Conversely, some may not require corrective actions because of the existence of compensating controls.

For security reasons, specifics concerning the potential vulnerabilities we identified are not discussed in this report. They are categorized as high, medium, and low potential vulnerabilities. High vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands on a web server. Medium and low vulnerabilities may provide an attacker with useful information, such as password files, to compromise DOT computers.

While all the potential vulnerabilities we identified need to be examined for possible actions, DOT and its Operating Administrations should correct the following as a priority.

---

[1] DOT had about 280 web servers as of May 15, 2001. Due to time-criticality, our scanning did not include all DOT web sites and was not designed to identify all potential vulnerabilities on DOT web servers.

- **The 68 high potential vulnerabilities**. Most of the high potential vulnerabilities we identified need to be corrected, some of which have to be fixed with software provided by computer manufacturers. Among these potential vulnerabilities, 26 were associated with the "Top Ten Internet Security Threats" issued by the Federal Chief Information Officers Council and should be eliminated immediately.

- **The medium vulnerabilities on four specific web servers**. Among the 42 medium potential vulnerabilities we identified, 4 enabled OIG to copy the password files from the web servers. These password files contain critical information, such as user and system administrator account names; network services; and DOT computer addresses, which could aid hackers.

- **The 23 low potential vulnerabilities identified last year but not fixed**. Among the 64 low potential vulnerabilities we identified, 23 had been previously identified by OIG for correction. These 23 potential vulnerabilities allowed access to DOT computers through special network services. While they are individually rated as low potential vulnerabilities, most co-exist with high or medium potential vulnerabilities on the same web server. Such a combination could provide easy paths for hacking exploitations and should be examined to determine whether or not compensating controls are in place. If not, corrective actions must be taken to mitigate the risks.

In our computer network security report,[2] we concluded that potential web vulnerabilities were caused by weak configuration management controls over web servers. The Office of the Chief Information Officer agreed to develop a "checklist" that the DOT Operating Administrations could use to perform self-certifications of their servers. The certification also would require concurrence by someone in the system owner's management chain that the web server is properly configured before the server could be put in use.

A draft checklist was sent to the Chief Information Officers Council Security Committee for comments on May 16, 2001. The DOT Deputy Chief Information Officer plans to finalize the checklist by May 31, 2001.

[2] Headquarters Computer Network Security, Report Number FI-2000-124, September 25, 2000.

RECOMMENDATIONS

To ensure timely corrections, we provided the specifics of all potential vulnerabilities we identified to the eight Operating Administrations and the DOT Deputy Chief Information Officer on May 4, 2001. We recommend that the DOT Deputy Chief Information Officer:

1. Establish June 8, 2001, as the deadline for Operating Administrations to correct all confirmed high, medium, and low potential vulnerabilities.

2. Expedite the issuance of the web configuration management controls checklist so that DOT Operating Administrations can certify the security of their web servers before releasing the servers for use.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Deputy Chief Information Officer on May 8, 2001. He concurred with the finding and recommendations. We considered his comments in preparing this report.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving your written comments within 30 days. If you concur with our finding and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of DOT representatives. If you have questions concerning this report, please call me at (202) 366-1992 or John Meche at (202) 366-1496.

-#-