Suncoast Technology Center

Security and Control
Incident Report

Incident ID: 10242006	Vulnerability: MS 02-039, Firewall Configuration	Exploit: SQL Slammer Worm	Date: 10/24/2006

Executive Summary:	An Internet service outage lasting approximately two hours occurred from 12:55pm to 2:46pm on Monday, 10/23/2006. The outage was caused by an unpatched database server that was compromised by a variant of the SQL Slammer worm. Once the server was infected, it sent traffic to other database severs on the Internet, and the traffic generated by the infected server rendered the firewall unavailable.
Background:	This incident was caused by three factors: an unpatched server, an insecure router / firewall configuration, and a NAT address assigned to a server without the server being scanned by the Security Team. 1. Unpatched Server The compromised server had a hostname of IFAS_SQL and an IP address of 10.140.20.89. It was found to be current on Operating System patches and Antivirus signatures, however the SQL Server 2000 application was completely unpatched. Essentially it was missing five years' worth of security updates. Among these updates is a patch for a buffer overflow vulnerability that was exploited by the SQL Slammer worm that hit in 2002. By means of comparison, the latest service pack for SQL 2000 is SP4, which was released on 5/6/2005. 2. Firewall / Router Configuration Checkpoint firewalls running on the SecurePlatform operating system have a known behavior of dropping routes when an interface goes down. At some point, the firewall lost the route to network 172.16.11.0, which is no longer a production network. However, the network object remained in the firewall, and the firewall rule that allows all internal networks to access any IP address on the ports the are allowed outbound did the opposite: it allowed any packets that had a forged source address on the 172.16.11 network to access internal hosts on any of the outbound ports. This is a common hacker technique called address spoofing, and is only successful in delivering a malicious payload over the UDP protocol. In this case, the permitted list of outbound ports includes port UDP 1433, the port used to query Microsoft SQL Servers. Likewise, the Admin Border Router has an Access Control List defined that blocks traffic from private addresses including 172.16 addresses. However, that access list is not applied to the internal and external interfaces. 3. NAT Address The IFAS_SQL server was never intended to be accessible from the public Internet. The Security Team assigned it a public NAT address of 204.193.127.168 in order to comply with EIT's support contract with our database support vendor, IT Convergence. Normally the Security Team does an additional audit on any server before giving it a NAT address. That audit did not happen in this case because the server was never intended for public access. In summary, these factors combined to create a situation where a hacker or virus could send UDP packets spoofed from the 172.16.11.0/24 network to public servers.

Description of Incident:	At 12:55 pm on 10/14/2006, a connection was made from 172.16.11.4 (spoofed) to IFAS_SQL. Immediately afterwards, IFAS_SQL flooded the firewall with outbound traffic going to random addresses on the internet using the standard SQL port of 1434. This traffic flooded the firewall state tables, which are responsible for maintaining the inbound and outbound traffic traversing the firewall. This lasted until 2:46 pm when the massive amount of traffic was observed in the firewall logs during troubleshooting. This can be noted in images "IFAS_SQL IN.jpg, IFAS_SQL OUT, and IFAS_SQL OUT2.jpg" Once the server was disconnected from the network and the firewall was brought back online, traffic resumed normally. During investigation of the machine, it was found that the SQL database administrator password had been changed to an unknown password. The Security Team also did an emergency change to remove the object for network 172.16.11.0, preventing this hole from being exploited by future attacks. Traffic from this spoofed address was also found to have been permitted to 10.140.60.28 (NAT 204.193.127.173), the Amanda production database server. A session was also attempted to 204.193.127.209, which does not have a server on it. See image "Other Connections.jpg". While recovering from this incident, EIT staff examined the Amanda database server and found it to be performing normally, sending no unusual traffic, and running a database server that is not vulnerable to the same vulnerability exploited on IFAS_SQL.
Corrective Action:	-Removed IFAS_SQL server from network. -Removed the 172.16.11.0 network from the firewall. -Had SysAdmins and DBA's scan 10.140.60.28 for any irregularities – no strange traffic seen in firewall logs. -DBA's are finding SQL instances where patch status is out of date.
Current Status of the Incident:	Connectivity has been restored, the server has been quarantined, and the hole has been closed.
Technical Recommendations:	Implement additional smart defense rule for massive UDP traffic to help detect and stop this type of traffic before it brings down the firewall. Locate servers where the OS and application updates are out of date and update as necessary. Add SQL and Oracle versions to the lists of apps to scan for during bi-weekly server scans.
Cost:	The cost of this incident comes from several sources: -Public downtime during the first day of early voting. -Lost productivity for the enterprise for approximately two hours of Internet downtime. -The time spent by 3 security members and 2 networking members to troubleshoot and investigate the problem.
Schedule:	All non-emergency changes have been postponed until after Election Day. They will be entered into Change Management during the week of November 6th.