Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory

April 29, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:
SA2009-025

DATE(S) ISSUED:
04/29/09

Subject:
Symantec Alert Management System 2 multiple vulnerabilities

Source:
Symantec

Systems Affected:
- SAV 9.0 MR6 and earlier
- SAV 10.0 all versions
- SAV 10.1 MR7 and earlier
- SAV 10.2 MR1 and earlier
- SEP 11.0 MR2 and earlier

Overview:
Alert Management System 2 (AMS2) is a component of the Symantec System Center console, Symantec AntiVirus Server, and of the Symantec AntiVirus Central Quarantine Server. AMS2 listens for specific security related events on a computer network, and sends notifications as specified by the administrator.

Four vulnerabilities in AMS2 components have been reported to Symantec.

1) **Intel Common Base Agent Remote Command Execution Vulnerability**
   The Intel LANDesk Common Base Agent (CBA) could allow a specially crafted packet sent to TCP Port 12174 to pass the packet contents as an argument to CreateProcessA(). The resulting command will be executed with SYSTEM privileges.

This vulnerability was discovered by Tenable Network Security, working through the Zero Day Initiative (ZDI).

2) **Intel Alert Originator Service Stack Overflow Vulnerability**
The Intel Alert Originator Service (IAO.EXE) does not properly validate data sent to a stack buffer through a call to memcpy(). An attacker could use a specially crafted packet to overflow the stack, and execute code of their choice with SYSTEM rights.

This vulnerability was discovered by: Sebastian Apelt, working through the Zero Day Initiative (ZDI).

3) **Intel Alert Originator Service Buffer Overflow Vulnerabilities**
Intel Alert Originator Service (IAO.EXE) does not properly validate data sent to it by the MsgSys.exe process. This could potentially lead to stack based buffer overflows during calls to strcpy() and memcpy(). An attacker could potentially leverage this to execute code of their choice with SYSTEM rights.

This vulnerability was discovered by Sebastian Apelt , working through the Zero Day Initiative (ZDI).

4) **Alert Management System Console Arbitrary Program Execution Design Error Vulnerability**
The Intel File Transfer service (XFR.EXE) provides file transfer capabilities to AMS2. A design error in XFR.EXE could allow an attacker to execute code of their choice with SYSTEM privileges on a vulnerable system. If an attacker is able to establish a TCP session with a vulnerable host, the issue could be exploited by placing arbitrary code on a fileshare or WebDav server, and then sending the UNC path to XFR.EXE. The code would then be executed on the vulnerable system.

Recommendations / Resolution:
Reporting has replaced AMS2 as the recommended method of alerting. Symantec Endpoint Protection Central Quarantine Server 11.0 MR3 and later no longer include AMS2. Symantec recommends that customers who are still using AMS2 switch to Reporting to manage alerts in their environments. If the customer is unable to switch to Reporting immediately then Symantec recommends that the customer either disables AMS2 as a temporary mitigation or completely uninstall AMS2.

References:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2009&suid=20090428_02