WHITE PAPER

INTEL-SA-00075 Network Administrator Detection and Mitigation Guide

Intel® Active Management Technology (Intel® AMT) and Intel® Standard Manageability (ISM).

Network Administrator Detection and Mitigation Guide for security vulnerability documented in INTEL-SA-00075

Revision 1.0 – May 12, 2017

Table of Contents

Executive Summary

Certain Intel manageability SKU systems are vulnerable to a known privilege escalation issue. This document identifies approaches that can be taken to utilize network filtering, monitoring, and packet inspection in response to the Intel manageability SKU systems privilege escalation issue. Read the Intel Public Security Advisory at https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr for more information.

Manageability Ports

Intel® Active Management Technology (Intel® AMT) and Intel® Standard Manageability (ISM) uses TCP/UDP messages addressed to certain registered ports. Messages received on a wired and wireless LAN interface and go directly to Intel® AMT and ISM. The following are the IANA registered ports that Intel® AMT / ISM may receive.

Port	Description	Details
16992	Intel® AMT HTTP	Used for WS-Management messages to and from Intel® AMT. This port is open over the network only when Intel® AMT is configured or during the configuration process. Starting with Release 6.0, the port is optionally open when TLS is enabled. The port is always open locally. See Defining Secure Connection Settings.
16993	Intel® AMT HTTPS	Used for WS-Management messages to and from Intel® AMT when TLS is enabled. See Transport Layer Security.
16994	Intel® AMT Redirection/TCP	Used for redirection traffic (SOL, Storage Redirection, and KVM using Intel® AMT authentication). Enabling the redirection listener enables this port. See Enabling the Listener State.
16995	Intel® AMT Redirection/TLS	Used for redirection traffic (SOL, Storage Redirection, and KVM using Intel® AMT authentication) when TLS is enabled. Enabling the redirection listener enables this port. See Enabling the Listener State.
623	ASF Remote Management and Control Protocol (ASF-RMCP)	Used for RMCP pings. This port is a standard DMTF port and accepts WS-Management traffic. It is always enabled.
664	DMTF out-of-band secure web services management protocol ASF Secure Remote Management and Control Protocol (ASF-RMCP)	Used for secure RMCP pings. This port is a standard DMTF port and accepts secure WS-Management traffic. It is always enabled.
5900	VNC (Virtual Network Computing) - remote control program	Used for KVM viewers that do not use Intel® AMT authentication but use the standard VNC port instead. See Working with Port 5900 and Changing the Default KVM Port Setting.

Additional details provided at https://software.intel.com/en-us/documentation/amt-reference/manageability-ports.

TCP/UDP network traffic filtering

In conjunction with implementing best known methods for securing network perimeter by blocking unused ports, additional network port filtering methods can be taken to actively filter manageability ports used by Intel® Active Management Technology (Intel® AMT) and Intel® Standard Manageability (ISM). The general approach would be to block incoming traffic targeting the ports used by Intel® AMT listed in the manageability port table.

There are several caveats and factors to consider before implementing this method:

- The packet filtering must be performed in the network, e.g. by managed switches, routers or gateways. Client host intrusion prevention system (HIPS) port filtering is not effective because the Intel® AMT services are accessed via an out-of-band network connection that does not go through the operating system network stack.
- If packet filtering is performed at managed switches and routers inside the network, it is likely to interfere with

legitimate use of Intel® AMT / ISM that originated from IT consoles inside the network.
- If packet filtering is performed at the network perimeter, consider that one compromised system inside the perimeter could still use the vulnerability to pivot and compromise other systems on the network. In this case the initial system would need to be compromised (which could occur via an unrelated method) and configured to behave as a rogue manageability console.
- Port based packet filtering at the network internal or perimeter only addresses the remote vulnerability. The local vulnerability would still remain and could be exploited if an attacker gained local, non-admin execution privileges on a targeted system.

Monitoring Manageability Port Traffic

Monitoring the network for unexpected Intel® AMT and ISM manageability traffic, over identified manageability ports, is one potential signal for identifying unauthorized use of manageability or use of the privilege escalation issue on identified Intel manageability SKUs. However, it will be necessary to differentiate traffic associated with legitimate use of Intel® AMT that originated from IT consoles inside the network. In those scenarios, it will be necessary to ignore / exclude verified source traffic from your network monitoring.

Please consult your network equipment manufacturing documentation or network intrusion detection & prevention system ISV on guides or templates on how to monitor for specific TCP/UDP source and port traffic.

Packet Inspection

IT departments can deploy IDS/IPS signatures to enable detection of CVE 2017-5689 exploitation attempts. This approach is only viable if manageability traffic to Intel® AMT or ISM is unencrypted over manageability port 16992/16994; encrypted manageability traffic over manageability port 16993/16995 will require the additional step of decryption to perform the packet inspection. Please consult your network intrusion detection & prevention system ISV on the method, if support, to implement this approach.

Understanding the IDS/IPS sensor placement is key to successful detection. Sensors need visibility into vulnerable system traffic. Lack of visibility will result in missed detections, such as exploitation attempts across the same VLAN. In addition, the Snort engine version will affect the rule options available for use and precision of detection. These payload strings can be adapted to other IDS/IPS engines that provide payload content matching and regular expressions.

Signature Rule 1 triggers upon an exploit attempt with a null 'response' value. This signature is keying from specific payload strings: content:"Authorization|3a 20|Digest", content:"response=", and a regular expression match of pcre:"/^\s*\x22{2}/R". Note that '|3a 20|' is hex representation for ': ' (colon space), and the regular expression is looking for two consecutive double-quote characters '""'.

This signature would only identify a zero-length response. It could be bypassed using an attack with a response having length greater than 0 (e.g. 1 character), which would not provide 100% success but would provide a much smaller search space to enable a brute force attack.

Signature Rule 1

Rule Description: Identify login with response = ""

Rule

```
alert tcp any any -> $HOME_NET
[16992:16995,623,664] (msg:"Sig1 Exploit:
CVE 2017-5689 HTTP NULL Digest
Authentication Bypass";
flow:to_server,established;
content:"Authorization|3a 20|Digest";
nocase; content:"username=|22|"; nocase;
distance:0; content:"response="; nocase;
distance:0; fast_pattern;
pcre:"/^\s*\x22{2}/R";
reference:url,mjg59.dreamwidth.org/48429.ht
ml;
reference:url,www.tenable.com/blog/rediscov
ering-the-intel-amt-vulnerability;
reference:cve,2017-5689;
classtype:attempted-admin; sid: 12345678;
rev:1;)
```

Signature Rule 2 uses a regular expression negative lookahead to enhance the detection. This lookahead functionality may not be supported in all Snort Engine implementations. This signature looks for similar content strings, but has a more complete regular expression with an explicit string negation (negative lookahead). This signature triggers upon a response value that is not followed by a 32 character string, and allows for whitespace between 'response', '=', and next string. This represents the null response string, but allowing for whitespace. This rule, like the rule above, is specified as 'any' to $HOME_NET which would allow detection of internal client exploitation as well as inbound traffic to Intel® AMT ports. Best practice would be to block inbound traffic to Intel® AMT ports, and so $EXTERNAL_NET exploitation attempts should not be seen. If

there is a business case for open Intel® AMT ports, the 'any' source variable would provide detection for exploitation.

Signature Rule 2

Rule Description: Identify login with incorrect response length

Rule

```
alert tcp any any -> $HOME_NET
[16992:16995,623,664] (msg:"Sig2 Exploit:
CVE 2017-5689: HTTP NULL Digest
Authentication Bypass";
flow:established,to_server; content:"|0D
0A|Authorization"; nocase; fast_pattern;
content:":"; within: 10;
content:"response"; nocase; distance:1;
pcre:"/response\s{0,10}=\s{0,10}[\"\'](?![a
-fA-F0-9]{32}[\"\'])[^\'\"]{0,128}[\"\']/";
reference:url,mjg59.dreamwidth.org/48429.ht
ml;
reference:url,www.tenable.com/blog/rediscov
ering-the-intel-amt-vulnerability;
reference:cve,2017-5689;
classtype:attempted-admin; sid: 12345679;
rev:1;)
```