What is the security issue?

The issue within Intel Active Management Technology (AMT), which is commonly found in most corporate laptops, allows an attacker to take complete control over a user’s device in a matter of seconds. The issue potentially affects millions of laptops globally.

A BIOS password normally prevents an unauthorized user from making low-level changes to a device. However, the essence of this issue is that even when a BIOS password has been set, an attacker does not need it to configure AMT. Not only that, due to insecure defaults in the BIOS and AMT’s BIOS extension (MEBx) configuration, an attacker with physical access can effectively backdoor a machine by provisioning AMT using the default password. The attacker can then access the device remotely, by connecting to the same wireless or wired network as the user. In certain cases, the assailant can also program AMT to connect to their own server, which negates the necessity of being in the same network segment as the victim.

No other security measures (full disk encryption, local firewall, anti-malware software or VPN) are able to prevent exploitation of this issue.

What is Intel Active Management Technology (AMT)?

AMT is Intel’s proprietary solution for remote-access monitoring and maintenance of corporate grade personal computers, created to allow IT departments or managed service providers to better control their device fleets. It gives a system administrator the opportunity to conduct difficult IT-related tasks over the wire by remotely connecting to a machine and taking over control from the user. Because it’s not tied to the operating system, AMT works even when the computer is turned off, as long as the device is connected to power and has a network cable attached.

AMT can be found on computers with Intel vPro-enabled processors, in addition to workstation platforms based on specific Intel Xeon processors. As most corporate laptops use Intel’s technology, AMT can be found on the vast majority of company endpoints.

Why is this a security issue?

The issue allows a local intruder to completely bypass all security measures a user might have deployed, and backdoor almost any corporate laptop in a matter of seconds. After the initial attack, the remote administration feature of AMT offers KVM (keyboard, video, mouse) access to the device under attack. Based on F-Secure’s experiences, AMT is rarely, if ever, hardened with a secure password or completely disabled.
A successful attack leads to complete loss of confidentiality, integrity and availability. The assailant is able to read and modify all of the data and applications a user may have access to on their computer. The attacker can also install malware on the device, even at the firmware level.

Is this a vulnerability?

Technically this is not a vulnerability, but a combination of a default password, insecure default configuration, and unexpected behaviour.

Is this exploitable over the network?

The initial provisioning needs to be done locally, with physical access to the device in question.

How can this be exploited?

Intel Active Management Technology comes initially protected with the default password “admin.” If AMT is not configured (as is the case with the vast majority of corporate devices), the default password will allow an attacker with physical access to the system to enable and configure AMT.

Although the attack cannot be enacted remotely, the process is very simple and quick to complete. A simple distraction, giving an attacker a few seconds of access to the target’s laptop, is enough to successfully complete the hack. The assailant can also provision the attack using a programmed USB stick, unless USB provisioning has been disabled by the user.

The attack process is explained step-by-step below:

1. The attack starts by the assailant rebooting the target’s system and hitting CTRL-P during the boot-up process. This brings the attacker to AMT’s Management Engine BIOS extension.

2. Once they’re inside AMT, the attacker can log in with the default password “admin.” AMT will then request the assailant to input a new password, which they can later use to gain access to the system remotely.

3. After inputting the new password, the attacker configures AMT to allow remote network access. On default settings, user consent is required to establish the remote connection – the assailant can, however, completely disable this option from the “User Consent” configuration menu.

4. Usually access to AMT is restricted to wired (ethernet) connections, but the attacker can also enable wireless access by connecting to the wired network and logging into the web console. From there the assailant can switch on wireless management.
5. The attacker can now connect to the system remotely, as long as he is in the same network with the hacked device. The actual connection can be performed with the Intel Manageability Developer Tool Kit’s Manageability Commander Tool, by using the username admin and the previously set password. In certain cases, the assailsant can also program AMT to connect to their own server by using Client Initiated Remote Access (CIRA), which negates the necessity of being in the same network segment with the victim.

6. Once logged in, the system can be controlled with Virtual Network Computing system (VNC). The target’s system is fully compromised, with the attacker having the capability to read and modify all data and applications within the boundaries of the user’s access rights.

What can organizations do to mitigate the issue?

Organizations need to adjust the system provisioning process to include setting a strong AMT password, and disabling AMT completely if this is possible. When ordering new devices, a decision needs to be made whether to order the devices without AMT, AMT disabled by default, or to provision AMT before enrollment.

IT departments also need to go through all currently deployed devices and configure the AMT password or disable the functionality altogether. It is recommended to query the amount of affected devices remotely, and narrow the list of assets needing attention down to a more manageable number. For computers connected to a Windows domain, provisioning can be done with Microsoft System Center Configuration Manager.

If a computer’s AMT password is already set to an unknown value, the device should be considered suspect and appropriate incident response procedures should be initiated.

Firmware updates correcting the issue need to be installed on all affected devices as soon as they become available.

How about end users?

Contact your IT service desk to set up AMT properly, or disable it if possible. If you are in charge of managing your own devices, go through the steps detailed in the previous section.

Your screen may display flashing borders during remote management over AMT. Contact your organization’s IT department in case this happens.

Most importantly: Never leave your devices unmonitored in an insecure location! Physical access to a device offers plenty of opportunity for malicious tampering.
What are manufacturers doing about the situation?

F-Secure has notified Intel, all relevant device manufacturers and CERT-CC about the security issue. Intel has produced a [Q&A about security best practices for AMT](#). For further comment on the issue, contact Intel or your respective device manufacturer.

Why have you come out with this?

This issue has no CVE number, security update or new version available, yet it affects major vendors and large numbers of laptops. AMT has gained popularity over the past few years, and only the latest security guides from Intel highlight the importance of requiring a BIOS password for local provisioning.

We have encountered this issue time and time again, and it is locally exploitable in practical situations even when laptops have otherwise been completely hardened. In other words, while Intel has written extensive guides on AMT, they have not had the desired impact on the real world security of corporate laptops.

With this announcement our goal is to raise awareness so organizations can have the opportunity to mitigate the issue and improve security in the real world.