computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-002

INTEL AMT Security Issue

January 12, 2018 — v1.0

History:

- *12/01/2018 — v1.0: Initial publication*

Summary

On January 12th 2018, F-Secure reported a security issue affecting laptops supporting Intel's Active Management Technology (AMT) [1]. The issue allows an attacker with physical access to the laptop to bypass the need to enter credentials, including BIOS and Bitlocker passwords and TPM pins, and to gain remote access for later exploitation.

The flaw described is caused by a weak default configuration on Intel Management Engine BIOS Extension (MEBx). The BIOS extension is accessible even if a password is set up for the BIOS.

Technical Details

Intel AMT is a 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.

The Intel Management Engine BIOS Extension (MEBx) can be accessed by pressing `CTRL-P` during bootup. The default password is `admin`. If unchanged, The attacker then can change the default password, enable remote access and set AMT's user opt-in to `None`. The attacker can now access the laptop if connected to the same network segment from wired or wireless networks.

Recommendations

If AMT is not needed, deactivate it in the BIOS configuration.

If it is needed, change the default password to a strong one – following the password policy in place.

References

[1] https://press.f-secure.com/2018/01/12/intel-amt-security-issue-lets-attackers-bypass-login-credentials-in-corporate-laptops/