预警编号：YJ-2018005

恒安嘉新

关于 Intel AMT 存在高危漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 1 月 16 日

1 漏洞描述

近期，互联网爆出 Intel AMT 存在高危安全漏洞。攻击者利用该漏洞可以完全控制目标用户的笔记本电脑。该漏洞危害程度为高危(High)。

2 影响范围

漏洞存在于英特尔（Intel） AMT 主动管理技术，针对笔记本电脑产品，尤其搭载英特尔企业级 vPro 处理器产品。

3 漏洞原理

Intel AMT，全称 INTEL Active Management Technology(英特尔主动管理技术) ,实质上是一种集成在芯片组中的嵌入式系统 ,独立于特定操作系统。该技术允许管理者远程管理和修复联网的计算机系统 ,且实施过程对服务对象完全透明。

该漏洞存在于 Intel AMT 主动管理技术，导致即使采用诸如 BIOS 密码，BitLocker，TPM Pin 或传统防病毒软件等安全措施，该漏洞依然可被利用。综合利用漏洞，攻击者可借助 Intel 管理引擎 BIOS 扩展(MEBx)默认密码“admin”功能进行登录，获取系统完全控制权限，窃取数据、还可在设备上部署恶意软件。区别于 Meltdown 和 Spectre，成功利用此漏洞（尚未命名）需要物理访问设备。

漏洞攻击场景如下：

（1） 攻击者需要本地对计算机进行操作；

（2） 重启上述笔记本电脑，进入启动菜单，通过使用英特尔管理引擎 BIOS 扩展（MEBx）功能，即默认密码“admin”登录；

（3） 修改上述（2）中默认密码，启用远程访问，并将 AMT 用户选择加入‘无’来有效地破坏机器。此外，有关研究表示，攻击者可将所使用 IP 插入与目标用户相同的网段进行远程访问。

4 修复建议

目前，Intel 厂商还未给出回应，建议大家可以先采用以下临时解决方案：

广大用户要加强对计算机资产的安全管理，且修改 AMT 默认密码为高复杂强度密码，或禁用 AMT 默认密码功能。