

漏洞相关信息

漏洞编号: CVE-2020-1301

漏洞名称: SMB v1远程代码执行漏洞

产品型号及版本: iMC_1.0系列产品, U-Center1.0系列产品 漏洞描述

漏洞描述

近日, 微软发布补丁修复了一个标注为远程代码执行的SMB v1漏洞: CVE-2020-1301, 漏洞影响Win7-Win10的所有版本。经分析, 该漏洞发生在srv驱动模块解析SMB相关协议MS-FSCC中的FSCTL_SIS_COPYFILE请求时, 没有完全验证请求中的SI_COPYFILE结构, 后续引用造成了整形溢出。与之前的SMBGhost (SMBv3漏洞) 相比, 该漏洞出现在老版本的SMB v1中, 触发需要先通过身份认证, 危害等级低于CVE-2020-0796。同时建议关闭SMB v1, 由于SMB v1存在很多安全问题, 如之前的永恒之蓝就是利用SMB v1漏洞。从2007年开始, SMB v2 和更高版本的协议取代了SMB v1。Microsoft在2014年公开弃用了SMB v1 协议。Windows 10已默认关闭SMB v1, 禁用SMB v1不会对系统造成影响。

漏洞解决方案

iMC&U-Center1.0系列皆不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响iMC&U-Center1.0功能

。

