安全漏洞通告

Windows MS-EFSRPC 协议 Ntlm Relay 攻击通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	Windows MS-EFSRPC 协议 Ntlm Relay 攻击通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072702
报告版本	1	报告日期	2021-07-27
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-27	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 27 日，360CERT 监测发现 Microsoft 发布了 缓解Windows域内证书服务Ntlm中继攻击 的风险通告，漏洞等级：严重，漏洞评分：9.8。

MS-EFSRPC 是 Microsoft 的加密文件系统远程协议，用于对远程存储和通过网络访问的加密数据进行维护和管理。

攻击者利用该漏洞可使域控制器使用 MS-EFSRPC 接口对远程 NTLM 服务器进行身份验证并共享其身份验证信息，从而允许攻击者发起 NTLM 中继攻击并完全接管 Windows 域。

对此，360CERT 建议广大用户做好资产自查以及预防工作，以免遭受黑客攻击。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
攻击者价值	高
利用难度	低
360CERT 评分	9.8

3 漏洞详情

3.1 ADV210003: Windows MS-EFSRPC 协议 Ntlm Relay 攻击

编号: ADV210003

组件: Windows Server

漏洞类型: Ntlm Relay

影响: 接管 windows 域

简述: 攻击者利用该漏洞可使域控制器使用 MS-EFSRPC 接口对远程 NTLM 服务器进行身份验证并共享其身份验证信息，从而允许攻击者发起 NTLM 中继攻击并完全接管 Windows 域。

目前 360CERT 已经复现该漏洞:

4 影响版本

组件	影响版本	安全版本
windows server	2008	暂无
windows server	2012	暂无
windows server	2016	暂无
windows server	2019	暂无
windows server	20H2	暂无
windows server	2004	暂无

5 修复建议

5.1 通用修补建议

目前该漏洞暂无官方补丁，官方推荐使用以下方式进行防御：

1. 微软建议客户在域控制器上禁用 NTLM 身份验证。

2. 如果处于业务原因无法关闭 NTLM，也可采取以下两个步骤的任意一个来缓解影响：

- 使用组策略在域中的任何 AD CS 服务器上禁用 NTLM

- 在运行CertificateAuthorityWebEnrollment 或者CertificateEnrollmentWebService服务的域中的 AD CS 服务器上禁用 Internet 信息服务 (IIS) 的 NTLM

6 时间线

2021-07-27 360CERT 发布通告

7 参考链接

https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360AISA 全流量威胁分析系统

针对微软本次安全更新，360AISA 已基于流量侧提供对应检测能力更新，请 AISA 用户联系 techsupport@360.cn 获取更新，尽快升级检测引擎和规则，做好安全防护工作。

A.2 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。