[系统安全] 十.Windows漏洞利用之SMBv3服务远程代码执行漏洞（CVE-2020-0796）及防御详解

原创

Eastmount 于 2020-12-30 15:13:36 发布 2876 收藏 15
分类专栏： 系统安全与恶意代码分析 文章标签： 网络安全 CVE-2020-0796 SMBv3 Web渗透 CVE复现

本文链接：https://blog.csdn.net/Eastmount/article/details/111518785
版权

系统安全与恶意代码分析 专栏收录该内容

50 篇文章 3 订阅 ¥9.90 ¥99.00
订阅专栏

您可能之前看到过我写的类似文章，为什么还要重复撰写呢？只是想更好地帮助初学者了解病毒逆向分析和系统安全，更加成体系且不破坏之前的系列。因此，我重新开设了这个专栏，准备系统整理和深入学习系统安全、逆向分析和恶意代码检测，"系统安全"系列文章会更加聚焦，更加系统，更加深入，也是作者的慢慢成长史。换专业确实挺难的，逆向分析也是块硬骨头，但我也试试，看看自己未来四年究竟能将它学到什么程度，漫漫长征路，偏向虎山行。享受过程，一起加油~

系统安全系列作者将深入研究恶意样本分析、逆向分析、攻防实战和Windows漏洞利用等，通过在线笔记和实践操作的形式分享与博友们学习，希望能与您一起进步。前文介绍了MS08-067远程代码执行漏洞（CVE-2008-4250），它是Windows Server服务RPC请求缓冲区溢出漏洞，利用445端口。这篇文章将详细讲解SMBv3服务远程代码执行漏洞（CVE-2020-0796），攻击者可能利用此漏洞远程无需用户验证，通过发送构造特殊的恶意数据导致在目标系统上执行恶意代码，从而获取机器的完全控制，利用的端口仍是445。希望对入门的同学有帮助。

话不多说，让我们开始新的征程吧！您的点赞、评论、收藏将是对我最大的支持，感恩安全路上一路前行，如果有写得不好的地方，可以联系我修改。基础性文章，希望对您有所帮助，作者的目的是与安全人共同进步，加油！也强烈推荐大家去看看参考文献的视频和书籍。

文章目录