河南省教育信息安全监测中心

梭子鱼邮件安全网关存在超危漏洞的风险预警

2023 年 6 月 8 日

梭子鱼邮件安全网关存在超危漏洞的风险预警

事件描述

近日，有关单位报，美国梭子鱼网络公司邮件安全网关产品存在命令注入超危漏洞，攻击者利用该漏洞可远程获取邮件安全网关的控制权限。目前，该公司已发布该漏洞修复补丁。

漏洞详情

影响版本 5.1.3.001-9.2.0.006 的梭子鱼电子邮件安全网关（仅限设备外形）产品中存在远程命令注入漏洞。 该漏洞是由于未能全面清理 .tar 文件（磁带存档）的处理而产生的。 该漏洞源于用户提供的 .tar 文件的不完整输入验证，因为它与存档中包含的文件的名称有关。 因此，远程攻击者可以以特定方式专门格式化这些文件名，从而导致通过 Perl 的 qx 运算符以电子邮件安全网关产品的权限远程执行系统命令。

漏洞编号

CVE-2023-2868

安全建议

请各地各单位高度重视，排查本单位是否使用梭子鱼邮件安全网关产品，及时修复漏洞，并排查处置遭攻击情况。重要情况及时报告省监测中心。

此问题已作为 BNSF-36456 补丁的一部分得到修复。此补丁已自动应用于所有客户设备。官方补丁下载地址：https://www.barracuda.com/company/legal/esg-vulnerability

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052