黑客利用VMware ESXi漏洞大肆攻击：数千台服务器被勒索软件攻击

2 月 7 日消息，根据报道，意大利国家网络安全局（ACN）于上周日发布警告，已经有黑客利用 VMware ESXi 服务器漏洞，对全球数千台服务器发起勒索软件攻击，并警告组织采取行动保护其系统。

ACN 总干事罗伯托·巴尔多尼（Roberto Baldoni）告诉路透社，黑客本次利用 VMware ESXi 服务器漏洞发起了大规模攻击。IT之家阅读了相关的报告，发现仅在意大利，每小时约有 20 台服务器受到攻击，数十家组织已经成为大规模网络犯罪活动的受害者。

CERT-FR

veille, d'alerte et de réponse aux attaques informatiques

用于监视、警报和响应计算机攻击的政府中心

PUBLICATIONS SERVICES ARCHIVES RÉSEAUX DE CSIRT RECRUTEMENT CONTACT À PROPOS

« précédent « 以前的

le 03 février 2023 2023 年 2 月 3 日

BULLETIN D'ALERTE DU CERT-FR CERT-FR 警报公告

Objet: [MàJ] Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi

主题：[更新] 影响 **VMware ESXi** 的漏洞利用活动

GESTION DU DOCUMENT 文件管理

Référence 参考	CERTFR-2023-ALE-015 CERTFR-2023-ALE-015
Titre	[MàJ] Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi [更新] 影响 VMware ESXi 的漏洞利用活动
Date de la première version 首次发布日期	03 février 2023 2023 年 2 月 3 日
Date de la dernière version 最新版本日期	05 février 2023 2023 年 2 月 5 日
Source(s) 来源	Bulletin de sécurité VMware VMSA-2021-0002 du 23 février 2021 2021 年 2 月 23 日发布的 VMware 安全公告 VMSA-2021-0002 Bulletin de sécurité VMware VMSA-2020-0023 du 20 octobre 2020 VMware 安全公告 VMSA-2020-0023 2020 年 10 月 20 日
Pièce(s) jointe(s) 附件)	Aucune(s) 没有任何

Tableau 1: Gestion du document 表 1：文档管理

Une gestion de version détaillée se trouve à la fin de ce document.

详细的版本管理可以在本文档的末尾找到。

预估本次大规模攻击中会有超过 500 家企业受到影响，其中法国企业受影响最大。该漏洞编号为 CVE-2021-21974，法国国家政府计算机安全事件响应小组 CERT-FR 已确认可以执行半自动攻击。

VMware 官方已经证实 VMware 的这个漏洞最早可以追溯到 2021 年年初，不过在 2021 年的 2 月已经发布补丁进行修复。

本文链接：https://dqcm.net/zixun/16757717437444.html