网址：[300,000 MikroTik routers are ticking security time bombs, researchers say | Ars Technica](https://arstechnica.com/information-technology/2021/12/300000-mikrotik-routers-are-ticking-security-time-bombs-researchers-say/)

# 原文：

# 300,000 MikroTik routers are ticking security time bombs, researchers say

## Device owners have yet to install patches for 3 high-severity vulnerabilities.

## As many as 300,000 routers made by Latvia-based MikroTik are vulnerable to remote attacks that can surreptitiously corral the devices into botnets that steal sensitive user data and participate in Internet-crippling DDoS attacks, researchers said.

The estimate, made by researchers at security firm Eclypsium, is based on Internet-wide scans that searched for MikroTik devices using firmware versions known to contain vulnerabilities that were discovered over the past three years. While the manufacturer has released patches, the Eclypsium research shows that a significant proportion of users has yet to install them.

“Given the challenges of updating MikroTik, there are large numbers of devices with these 2018 and 2019 vulnerabilities,” Eclypsium researchers [wrote in a post](https://eclypsium.com/2021/12/09/when-honey-bees-become-murder-hornets/). “Collectively, this gives attackers many opportunities to gain full control over very powerful devices, positioning them to be able to target devices both behind the LAN port as well as target other devices on the Internet.”

## Embraced by script kiddies and nation-states alike

## The concern is far from theoretical. In early 2018, researchers at security firm Kaspersky said that a powerful nation-state malware called Slingshot, which had gone undetected for six years, [initially spread through MikroTik](https://arstechnica.com/information-technology/2018/03/potent-malware-that-hid-for-six-years-spread-through-routers/) routers. The attacks downloaded malicious files from vulnerable routers by abusing a MikroTik configuration utility known as Winbox, which transferred the payloads from the device file system to a connected computer.

A few months later, researchers at security firm Trustwave discovered [two malware campaigns](https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/mass-mikrotik-router-infection-first-we-cryptojack-brazil-then-we-take-the-world/) against MikroTik routers after reverse engineering a CIA tool leaked in a [WikiLeaks series known as Vault7](https://arstechnica.com/information-technology/2017/04/found-in-the-wild-vault7-hacking-tools-wikileaks-attributes-to-the-cia/).

Also in 2018, China's Netlab 360 [reported](https://arstechnica.com/information-technology/2018/09/unpatched-routers-being-used-to-build-vast-proxy-army-spy-on-networks/) that thousands of MikroTik routers had been swept into a botnet by malware attacking a vulnerability tracked as CVE-2018-14847.

The Eclypsium researchers said that CVE-2018-14847 is one of at least three high-severity vulnerabilities that remains unpatched in the Internet-connected MikroTik devices they tracked. Combined with two other vulnerabilities located in Winbox—[CVE-2019-3977](https://arstechnica.com/information-technology/2021/12/300000-mikrotik-routers-are-ticking-security-time-bombs-researchers-say/%E2%80%8B%E2%80%8Bhttps://nvd.nist.gov/vuln/detail/CVE-2019-3977) and [CVE-2019-3978](https://nvd.nist.gov/vuln/detail/CVE-2019-3978)—Eclypsium found 300,000 vulnerable devices. Once hackers infect a device, they typically use it to launch further attacks, steal user data, or participate in distributed denial-of-service attacks.

The researchers have released a [free software tool](https://github.com/eclypsium/mikrotik_meris_checker) that people can use to detect if their MikroTik device is either vulnerable or infected. The company also provides other suggestions for locking down the devices. As always, the best way to secure a device is to ensure it’s running the latest firmware. It’s also important to replace default passwords with strong ones and turn off remote administration unless it’s necessary.

译文：

题目：

研究者：“300000个MikroTik生产的路由器正在安置定时安全炸弹。”

——设备拥有者目前需要安装补丁程序来修复三个严重漏洞

正文：

研究者称有三万个由总部设置在拉脱维亚的MikroTik厂商生产的路由器目前被发现容易受到能够秘密地把设备拖入可以窃取用户敏感数据的僵尸网络并导致产生互联网瘫痪以及分布式拒绝服务攻击（DDoS attack)的远程攻击。这项评估是由安全公司Eclypsium的研究者完成的。他们使用了一项互联网电子扫描技术，搜查到了MikroTik厂家的设备使用了一个目前已知携带有漏洞的固件版本，而这些漏洞在三年前就已经被发现了。在厂家发布了补丁程序后，研究者们观察到有非常大一部分的用户已经下载了这一补丁程序。

“鉴于MikroTik在升级版本的过程中遭遇到的困难，有大批量的设备携带有2018和2019这两年发布的版本的漏洞。”Eclypsium的研究者在他们的研究报告中如是写道，“而当这些设备被集中起来的时候，就给了攻击者大量的机会来获取对于高效能的设备的完全控制权，并安置这些设备来攻击那些在局域网端口（LAN port后的设备以及那些其他联网的设备。

受到互联网黑客和国民的欢迎

对这些设备的关注早已不止于理论层面了。早在2018年，来自安全公司Kaspersky的研究者们说一种名为“Slingshot”流行于国民中的高效能的恶意软件已经潜伏六年还未被发现，而这一恶意软件最初就是通过MikroTik生产的路由器传播的。这种软件的攻击方式是通过滥用MikroTik配置的实用程序“Winbox”从易受攻击的路由器下载恶意文件，这样便把设备的文件系统的有效载荷全部转移到了设备连接到的电脑上。几个月前，来自安全公司Trustware的研究者们发现了在MikrotiK的路由器使用了中情局提供的工具后，有两次恶意活动泄露到了维基解密（WikiLeaks）系列的Vault7中。也是在2018年，中国的360网络实验室报告称有数以千计的MikroTik生产的路由器已经被一个最易受攻击的路由器CVE-2018-14847通过恶意袭击扫荡进了僵尸网络中。

来自Eclypsium的研究者们说路由器CVE-2018-14847中至少存在着他们目前跟踪的所有能够联网的MikroTik设备中未被补丁的三个严重漏洞中的一个。通过结合其他两个设置在“Winbox”中的易受攻击路由器CVE-2019-3977和路由器CVE-2019-3978，Eclypsium的研究者们发现了300000个易受攻击的设备。一旦黑客控制了其中的一个，他们通常就会利用它来展开更进一步的攻击，比如窃取用户的数据，或者开展分布式拒绝服务攻击（DDoS attack)。

研究者们已经发布了一个免费的软件工具，人们可以使用它们来检查自己的MikroTik设备是否是易受到攻击的或是已经被攻击的。这家公司也提供了一些其他的意见来封锁这些设备。众所周知，保障一台设备安全的最佳措施就是确保它运行在最新版本的固件上。同时，把默认的密码换成安全性更强的密码并且在除非是必要的情况下关闭远程控制也是很重要的。