UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: DigitalOcean

UNIVERSITAS GADJAH MADA

Date: 27 June 2024
Version 1.0

Introduction

This is a pentesting report for CVE-2018-14847. CVE-2018-14847 is a vulnerability in the Winbox component of MikroTik RouterOS. The vulnerability allows an unauthenticated remote attacker to execute arbitrary code on vulnerable routers. The impact of this vulnerability includes unauthorized access to the router, data theft, and potential network compromise. It is crucial to address this vulnerability promptly to protect the security and integrity of the network infrastructure.

Executive Summary

Number of Vulnerable Devices: 3

Number of Exploitable Devices: 0

Number of Extracted Credentials: 0

The executive summary provides an overview of the findings and key statistics related to the penetration testing performed. It highlights the number of vulnerable devices, exploitable devices, and the count of extracted credentials. These metrics help in assessing the severity and impact of the identified vulnerability and provide an initial understanding of the security posture of the network infrastructure.

Findings

Vulnerable Devices

Detected devices that are vulnerable to CVE-2018-14847:

192.81.221.22	DigitalOcean, LLC	MikroTik RouterOS 6.37rc35	2024-06-19T22:32:07.391533
138.197.3.249	DigitalOcean, LLC	MikroTik RouterOS 6.37rc35	2024-06-06T20:42:14.630370
128.199.137.13	DigitalOcean, LLC	MikroTik RouterOS 6.40.9	2024-06-25T10:45:26.822549

Exploitable Devices

Credential dumped from exploitable devices:

Target: 192.81.221.22

Target: 138.197.3.249

Target: 128.199.137.13

Target: 192.81.221.22

Target: 138.197.3.249

Target: 128.199.137.13

Recommendation

To mitigate CVE-2018-14847, it is recommended to take the following steps:
- Update the MikroTik RouterOS to the latest version available.
- Apply firewall rules to restrict access to the Winbox service.
- Regularly monitor and review logs for any suspicious activity.
- Implement strong password policies and avoid using default credentials.
- Keep the network infrastructure and devices up to date with security patches.
- Conduct regular security assessments and penetration testing to identify vulnerabilities.