

# MikroTik WinBox Path Traversal





















Medium

[← View More Research Advisories](#)

## Synopsis

MikroTik WinBox before 3.21 is vulnerable to a path traversal issue that allows an attacker to write files anywhere on the system where WinBox has write privileges.

When WinBox connects to a router, it downloads the `list` file from `/home/web/webfig/`. This file contains a list of files that WinBox should download in order to obtain package descriptions. WinBox downloads these files and stores them on the client's system within the MikroTik roaming directory: `C:\Users\[username]\AppData\Roaming\Mikrotik\Winbox`.

s > REBox > AppData > Roaming > Mikrotik > Winbox > 6.44.6-1806017272				
Search 6.44.6-1806017272				
Name	Date modified	Type	Size	
 advtool.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 advtool.jg	2/6/2020 6:28 AM	JG File	5 KB	
 dhcp.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 dhcp.jg	2/6/2020 6:28 AM	JG File	17 KB	
 hotspot.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 hotspot.jg	2/6/2020 6:28 AM	JG File	19 KB	
 icons.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 icons	2/6/2020 6:28 AM	PNG File	22 KB	
 mpls.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 mpls.jg	2/6/2020 6:28 AM	JG File	19 KB	
 ppp.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 ppp.jg	2/6/2020 6:28 AM	JG File	28 KB	
 roteros.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 roteros.jg	2/6/2020 6:28 AM	JG File	513 KB	
 rotating.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 rotating.jg	2/6/2020 6:28 AM	JG File	53 KB	
 secure.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 secure.jg	2/6/2020 6:28 AM	JG File	15 KB	
 wlan6.crc	2/6/2020 6:28 AM	CRC File	1 KB	
 wlan6.jg	2/6/2020 6:28 AM	JG File	111 KB	

The name of the created files come directly from the downloaded `list` file. For example, this is a line from `list`:

```
{ crc: 164562873, size: 1149, name: "advtool.jg", unique: "advtool-fc1932f6809e.jg", version: "6.39.3" }
```

WinBox will use the name "advtool.jg" as the filename in the roaming directory. However, WinBox doesn't do any type of checking for directory traversal on these files. So if presented with:

```
{ crc: 164562873, size: 1149, name: "..\\..\\..\\..\\..\\..\\Users\\Public\\lol.txt", unique: "advtool-fc1932f6809e.jg", version: "6.39.3" }
```

Then WinBox would create the file `C:\Users\Public\lol.txt` and fill it with contents provided by the attacker.

An attacker can exploit this bug by getting a victim to connect to a malicious MikroTik router, a fake router (see our [PoC](#) for CVE-2019-3981), or via a man in the middle attack. The attacker can then perform the downgrade attack described in [TRA-2020-01](#). The client will then try to download the files from the attacker.

A [proof of concept](#) has been uploaded to our research GitHub repository. The PoC listens on port 8291. When WinBox connects to it, the script will ignore the ECSRP message so that the client switches to Diffie-Hellman. After the login is complete, the script serves up a malicious list file and eventually writes the file `C:\Users\Public\lol.txt` with the contents "hello mikrotik".

## Solution

Upgrade to Winbox 3.21

## Additional References

<https://forum.mikrotik.com/viewtopic.php?f=21&t=157150>

## Disclosure Timeline

January 16, 2020 - Tenable discloses issue to MikroTik. 90 days is April 15, 2020.  
January 17, 2020 - MikroTik appears to indicate path traversal will be fixed when DH is fixed (no set date).  
January 17, 2020 - Tenable reiterates that the path traversal issue is separate from the DH problem.  
January 20, 2020 - Tenable and MikroTik exchange emails on RouterOS architecture.  
February 6, 2020 - Tenable notices a post on Reddit indicating WinBox 3.21 fixes the reported issues.

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*



## Risk Information

---

CVE ID: [CVE-2020-5720](#)

Tenable Advisory ID: TRA-2020-07

Credit: Jacob Baines

CVSSv2 Base / Temporal Score: 4.3 / 3.6

CVSSv2 Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Additional Keywords : CWE-22

Affected Products: MikroTik WinBox before 3.21

Risk Factor: Medium

## Advisory Timeline

---

February 6, 2020 - Initial Release

---

### FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

### FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

### CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

### CONNECTIONS

Blog

Contact Us

