

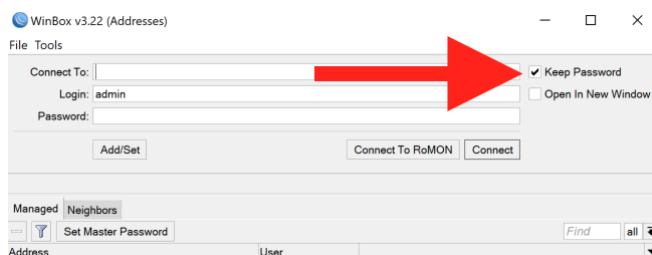
## MikroTik WinBox Cleartext Password Storage

Low

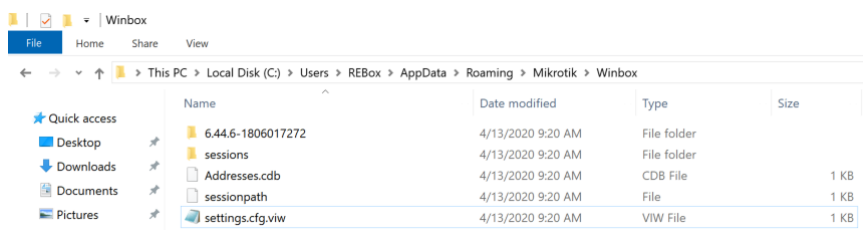
[← View More Research Advisories](#)

## Synopsis

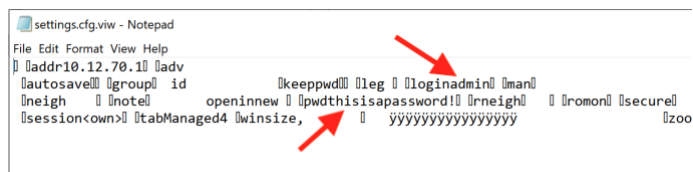
MikroTik's WinBox stores the user's cleartext password in a configuration file when the *Keep Password* option is selected. *Keep Password* is enabled by default.



Specifically, the password is stored in a file called *settings.cfg.viw* in Winbox's *AppData/Roaming* directory. The full path is *C:\Users\USERNAME\AppData\Roaming\Mikrotik\Winbox\settings.cfg.viw*



The username and password can be found appended to the keywords *login* and *pwd* respectively.



An attacker that gains access to this file can use it to pivot to the router.

## Solution

This issue affects all known versions of WinBox. However, to mitigate this issue, MikroTik suggests using WinBox's "Set Master Password" functionality.

## Additional References

<https://cwe.mitre.org/data/definitions/260.html>

<https://wiki.mikrotik.com/wiki/Manual:Winbox>

## Disclosure Timeline

01/16/2020 - Tenable discloses to MikroTik. 90 days is April 15, 2020.

01/17/2020 - MikroTik indicates that the plaintext password issue isn't an issue because users can encrypt the password through an additional mechanism.

01/17/2020 - Tenable reiterates that they believe plaintext password storage is an issue.

01/18/2020 - MikroTik states "By default, no credentials are being stored in settings.cfg..." MikroTik commits to adding additional info messages.

01/20/2020 - Tenable disagrees. By default Keep Password is set which causes the password to be saved. Tenable agrees additional information to the users would be good.

01/27/2020 - MikroTik replies with, "thank you for the suggestions."

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.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)

## Risk Information

CVE ID: [CVE-2020-5721](#)



CVSSv2 vector: AV:L/AU:L/AU:N/C:P/I:N/A:N

Additional Keywords : CWE-260

Affected Products: WinBox 3.22 and below

Risk Factor: Low

## Advisory Timeline

---

April 15, 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

Careers

Investors

Events

Media



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

