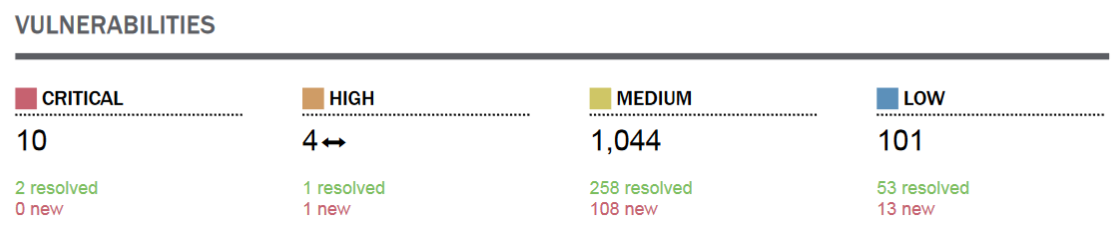
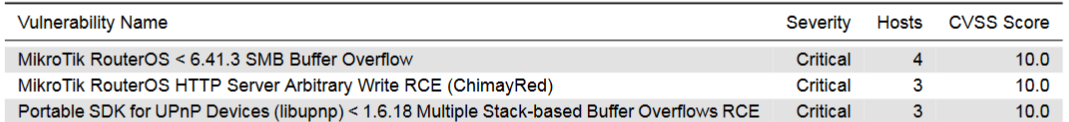
Hélio Ferreira 08/05/2024

LAB: CYBER RISK ANALYSIS

### **Part 1: Review the CyHy Report**

* Read through the CyHy Report and identify potential risks
  + Take notes as needed

According to the report , I’ve found 393 vulnerable Hosts , which contained 1159 vulnerabilities.   
  
  
Concerning vulnerabilities, 10 of them are considered Critical , 4 are High, 1,044 are Medium and 101 are Low.  
  
  
  
Speaking about the Critical ones:  
  
The first one:  
  
- It's a flaw in the SMB (Server Message Block) service of MikroTik RouterOS versions before 6.41.3.

- An attacker can exploit this by sending specially crafted messages to the SMB service, causing a buffer overflow.

- This overflow can then be used to inject malicious code and gain control of the router.

The second one:

- This flaw exists in MikroTik RouterOS versions before Stable 6.38.5 and Long-term 6.37.5.

- An attacker can exploit it by sending a specially crafted HTTP request to the router's web server.

- This malicious request can potentially overwrite memory locations on the router, allowing the attacker to execute arbitrary code and gain full control.

Finally, the third one:  
  
- It's a collection of security holes (stack-based buffer overflows) in libupnp versions before 1.6.18.

- libupnp is a popular library used by many devices to implement the Universal Plug and Play (UPnP) protocol.

- These vulnerabilities can be exploited by sending malicious data packets specifically crafted to overflow buffers within the libupnp code.

- This overflow can then be used to inject malicious code and potentially grant remote attackers full control of the affected device.

### **Part 2: Create the Risk Assessment Report**

* Using the provided Excel worksheet, populate the fields and submit the completed worksheet.  
    
  **https://docs.google.com/spreadsheets/d/1fM0lYxlbtm06Mtgv58eZzoa8A3mcQNiGcuVSo3u0Z\_k/edit?usp=sharing**
* What are the biggest cyber risks to Initrobe?  
    
  The Biggest cyber risks to Initrobe are the 3 Critical Ones.
  + Justify your reasoning.  
      
    **Ease of Exploitation:** This vulnerability allows for remote code execution (RCE) without any authentication required. An attacker can exploit this over the internet without needing any prior access to your router. This makes it very easy for attackers to target a large number of devices.

**High Impact:** Once exploited, an attacker can gain complete control over your MikroTik router. This can lead to devastating consequences, including:

**Data Breaches:** Attackers can steal sensitive information that flows through your network, such as login credentials, financial data, and personal communications.

**Network Disruptions:** Attackers can disrupt your network traffic by overloading the router, redirecting traffic, or launching denial-of-service (DoS) attacks. This can significantly impact your network's availability and functionality.

**Compromised Devices:** The compromised router can be used as a launchpad for further attacks on other devices within your network, potentially leading to a domino effect.

* + For each risk, what are at least two ways we could mitigate the risk?  
      
    Here are ways to mitigate the risks associated with the three vulnerabilities you mentioned:

**1. MikroTik RouterOS < 6.41.3 SMB Buffer Overflow (Critical 4 10.0):**

* **Patch Immediately:** This is the most crucial step. Update your MikroTik RouterOS to version 6.41.3 or later as soon as possible. This patch addresses the specific buffer overflow vulnerability. MikroTik typically releases updates that address security vulnerabilities. You can find the latest version and update instructions on the MikroTik website.
* **Disable SMB Service (Temporary Workaround):** If updating immediately isn't feasible, consider disabling the SMB service on your router as a temporary workaround. However, this might limit your ability to share files across your network.

**2. MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed) (Critical 3 10.0):**

* **Update MikroTik RouterOS:** While the risk might be slightly lower than the SMB overflow, updating your RouterOS to the latest stable version is still highly recommended. This will likely include patches for ChimayRed and other vulnerabilities.
* **Web Server Security:** Consider additional security measures for your MikroTik router's web server if possible. This could involve:
  + **Limiting Access:** Restrict access to the web interface to authorized users only, ideally from specific IP addresses.
  + **Strong Passwords:** Implement strong and unique passwords for accessing the router's web interface.

**3. Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE (Critical 3 10.0):**

* **Identify Vulnerable Devices:** Use device scanners or tools provided by your device vendor to identify any devices on your network that might be using a vulnerable version of libupnp.
* **Update Firmware:** If possible, update the firmware on your vulnerable devices to a version that includes a patched libupnp library. Consult the documentation or support channels of your device vendor for specific instructions.
* **Disable UPnP (if necessary):** On some devices, you might be able to disable UPnP functionality altogether as a temporary workaround. However, this might limit some functionalities, so check your device's manual for potential consequences.
  + For each risk, what is the most effective risk mitigation technique of the ideas you came up with? This should be the lowest cost and greatest mitigation.  
      
    - MikroTik RouterOS < 6.41.3 SMB Buffer Overflow (Critical 4 10.0):

Most Effective Technique: Patch MikroTik RouterOS Immediately  
 **-** MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed) (Critical 3 10.0):

Most Effective Technique: Update MikroTik RouterOS

**-** Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE (Critical 3 10.0):

Most Effective Technique: Identify Vulnerable Devices and Update Firmware

### **Part 3: Quantitative Deterministic Risk Calculation**

* For the **worst** case scenario:
  + Determine the AV, EF, and ARO. Justify your reasoning.  
    - AV =6.173.16,00  
    - EF= 30%  
    - ARO= 4

| AV (Asset Value) | EF (Exposure Factor) | ARO (Annual rate of occurrence) |
| --- | --- | --- |
| 6.173.160,00 | 30% | 0.25 |

* + Calculate the SLE. Explain and justify your method.  
    SLE - Single Loss Expectancy = AV\*EF
  + Calculate the ALE. Explain and justify your method.  
    ALE - Annualized Loss Expectancy = SLE\*ARO

| SLE (Single Life Expectancy) | ALE (Annualized Loss Expectancy) |
| --- | --- |
| 1.851.948,00 | 462.987,00 |

* For the **best** case scenario:
  + Determine the AV, EF, and ARO. Justify your reasoning.  
    - AV =6.173.16,00  
    - EF= 30%  
    - ARO= 4

| AV (Asset Value) | EF (Exposure Factor) | ARO (Annual rate of occurrence) |
| --- | --- | --- |
| 6.173.160,00 | 15% | 0,16 |

* + Calculate the SLE. Explain and justify your method.  
    SLE - Single Loss Expectancy = AV\*EF
  + Calculate the ALE. Explain and justify your method.  
    ALE - Annualized Loss Expectancy = SLE\*ARO

| SLE (Single Life Expectancy) | ALE (Annualized Loss Expectancy) |
| --- | --- |
| 925.974,00 | 148.155,84 |

* For the **most likely** scenario:
  + Determine the AV, EF, and ARO. Justify your reasoning.  
    - AV =6.173.16,00  
    - EF= 30%  
    - ARO= 4

| AV (Asset Value) | EF (Exposure Factor) | ARO (Annual rate of occurrence) |
| --- | --- | --- |
| 6.173.160,00 | 25% | 0.2 |

* + Calculate the SLE. Explain and justify your method.  
    SLE - Single Loss Expectancy = AV\*EF
  + Calculate the ALE. Explain and justify your method.  
    ALE - Annualized Loss Expectancy = SLE\*ARO

| SLE (Single Life Expectancy) | ALE (Annualized Loss Expectancy) |
| --- | --- |
| 1.543.290,00 | 308.658,00 |

* Create a table in your Google Doc submission of the calculated values for all three scenarios. Convert and present the monetary figures in USD for all fields of the table, and include the conversion rate used.  
    
  <https://docs.google.com/spreadsheets/d/1ohUbBA7hIihPzPcoGe05ZDbj93PtnWu5lPpn3eDGgbE/edit?usp=sharing>