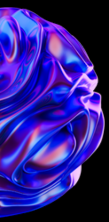
KORENIX JETIO 6550

WHEN THE ETHERNET I/O SERVER ROUTER SUCCUMBS TO EVIL.

CVE-2024-2371

HADESS

WWW.HADESS.IO



INTRODUCTION

In the realm of network security, vulnerabilities can present significant risks to the integrity and confidentiality of data. CVE-2024-2371, a vulnerability identified within Korenix JetIO, is a prime example of such a threat. Korenix JetIO is a popular industrial Ethernet switch series widely used in critical infrastructure and industrial control systems (ICS). This vulnerability, designated CVE-2024-2371, exposes these systems to potential exploitation by malicious actors. In this introduction, we delve into the intricacies of this vulnerability, exploring its nature, implications, and potential mitigations.

At the heart of CVE-2024-2371 lies a flaw in Korenix JetIO's handling of the Simple Network Management Protocol (SNMP). SNMP, a widely used protocol for network management, is leveraged by Korenix JetIO for various administrative tasks. However, the vulnerability allows an attacker to utilize SNMP to access sensitive data within the system. This presents a serious risk as sensitive data within industrial environments often includes critical operational information or confidential data.

The exploitation of CVE-2024-2371 poses significant threats to the affected systems. By leveraging SNMP, attackers can potentially gain unauthorized access to sensitive data, including configuration details, network topology information, and other critical parameters. In industrial settings, such data can be instrumental in orchestrating targeted attacks, disrupting operations, or even causing physical harm to equipment and personnel.

Moreover, the implications of CVE-2024-2371 extend beyond immediate data breaches. In industrial environments where uptime and reliability are paramount, any compromise to network security can lead to operational disruptions, financial losses, and reputational damage. Furthermore, given the interconnected nature of modern industrial systems, a breach in one component can cascade into broader system-wide vulnerabilities, amplifying the potential impact of the exploit.

The discovery of CVE-2024-2371 underscores the ongoing challenges in securing industrial control systems against evolving threats. As industrial networks increasingly adopt interconnected and digitized solutions, the attack surface for malicious actors continues to expand. Vulnerabilities such as CVE-2024-2371 highlight the critical need for robust security measures tailored to the unique requirements of industrial environments, including thorough risk assessments, timely patching, and effective intrusion detection systems.

Mitigating the risks associated with CVE-2024-2371 requires a concerted effort from stakeholders across various domains. Vendors of Korenix JetIO and similar industrial networking equipment must promptly release patches or firmware updates to address the vulnerability. Additionally, industrial operators should implement stringent access controls, segment networks, and employ intrusion detection systems to detect and thwart unauthorized access attempts. Collaborative initiatives within the cybersecurity community are also essential for sharing threat intelligence and best practices to fortify defenses against similar vulnerabilities in the future.

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.

DOCUMENT INFO

HADESS

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.

At Hadess, our mission is twofold: to unleash the power of white hat hacking in punishing black hat hackers and to fortify the digital defenses of our clients. We are committed to employing our elite team of expert cybersecurity professionals to identify, neutralize, and bring to justice those who seek to exploit vulnerabilities. Simultaneously, we provide comprehensive solutions and services to protect our client's digital assets, ensuring their resilience against cyber attacks. With an unwavering focus on integrity, innovation, and client satisfaction, we strive to be the guardian of trust and security in the digital realm.

TABLE OF CONTENT

Executive Summary

CVE-2024-2371 exposes a vulnerability in Korenix JetIO switches, affecting the Simple Network Management Protocol (SNMP) implementation. SNMP, a commonly used protocol for network management, is leveraged by Korenix JetIO switches for administrative tasks. However, the flaw allows unauthorized users to exploit SNMP to access sensitive data within the system.

The vulnerability arises due to insufficient access controls within the SNMP implementation of Korenix JetIO switches. Attackers can exploit this flaw to read sensitive data, including configuration details and network topology information. By sending crafted SNMP requests, malicious actors can bypass authentication mechanisms and gain unauthorized access to critical system parameters.

The exploitation of CVE-2024-2371 poses significant risks to industrial control systems (ICS) and critical infrastructure. Attackers could exploit this vulnerability to gather intelligence for targeted attacks, disrupt operations, or manipulate systems. Given the interconnected nature of industrial networks, the impact of a successful exploit could extend beyond individual systems, potentially affecting broader operational environments.

Mitigating the risks associated with CVE-2024-2371 requires prompt action from vendors and operators. Vendors should release patches or firmware updates to address the vulnerability, while operators should implement strict access controls, network segmentation, and intrusion detection systems. Collaboration within the cybersecurity community is crucial for sharing threat intelligence and best practices to enhance defenses against similar vulnerabilities in industrial environments.

https://www.incibe.es/en/incibe-cert/notices/aviso-sci/information-exposure-vulnerability-korenix-jetio-6550

Key Findings

- Information Exposure via SNMP protocol

Abstract

The Korenix JetIO vulnerability, identified as CVE-2024-2371, poses a significant risk to industrial control systems (ICS) and critical infrastructure. This vulnerability, arising from flaws in the implementation of the Simple Network Management Protocol (SNMP) within Korenix JetIO switches, allows unauthorized access to sensitive data. Leveraging SNMP, malicious actors can bypass authentication mechanisms and retrieve critical system parameters, including configuration details and network topology information.

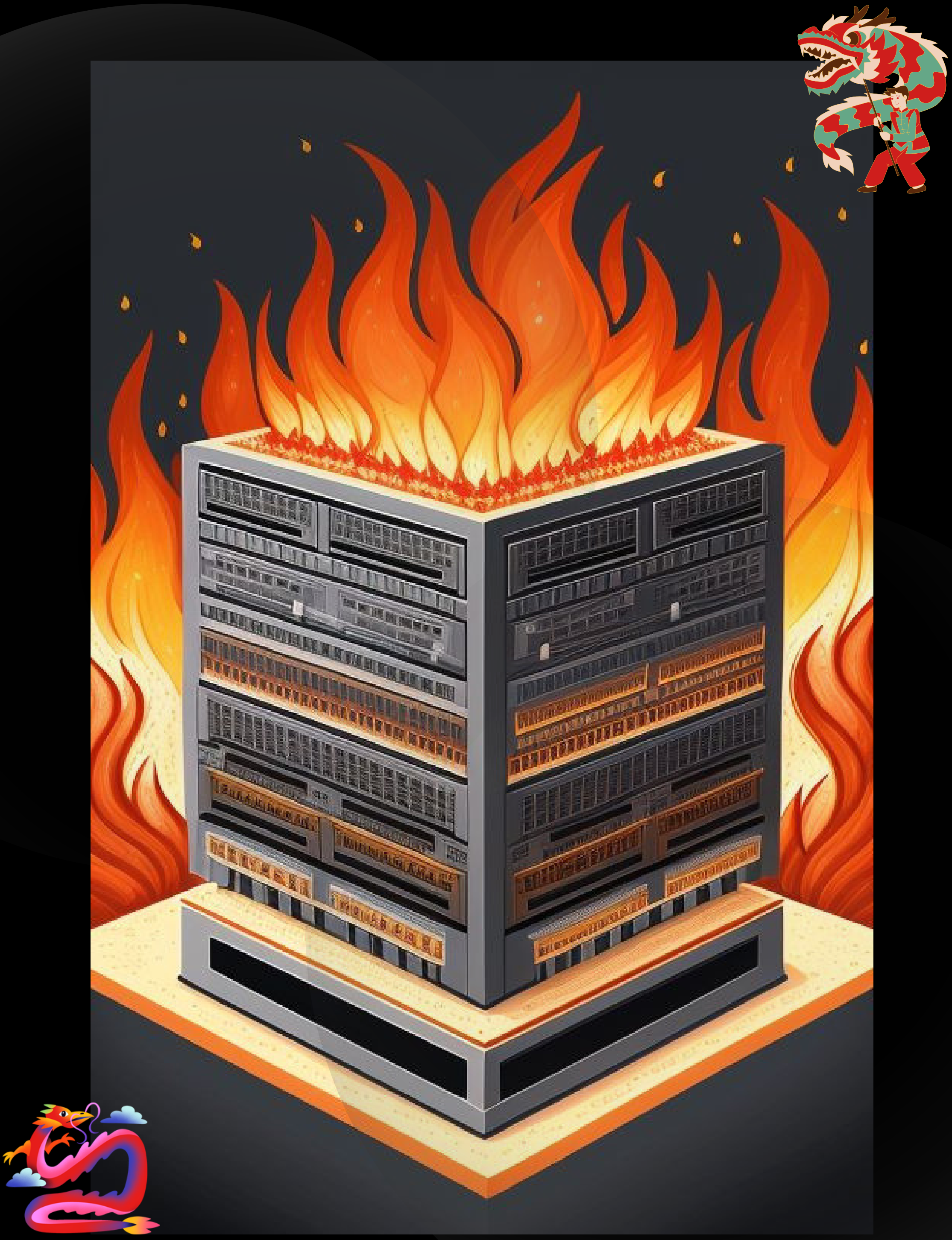
The exploitation of CVE-2024-2371 presents multifaceted threats to industrial networks. Attackers could exploit this vulnerability to gather intelligence for targeted attacks, disrupt operations, or manipulate systems, potentially causing physical harm to equipment and personnel. Given the interconnected nature of industrial systems, the impact of a successful exploit could cascade into broader operational disruptions and financial losses.

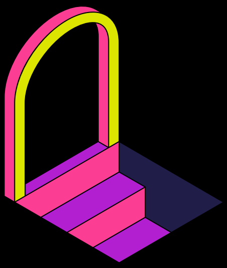
Addressing CVE-2024-2371 requires coordinated efforts from vendors and operators. Vendors must swiftly release patches or firmware updates to mitigate the vulnerability, while operators should implement stringent access controls, network segmentation, and intrusion detection systems. Additionally, collaborative initiatives within the cybersecurity community are essential for sharing threat intelligence and best practices to fortify defenses against similar vulnerabilities in industrial environments.

As the digitalization of industrial processes continues to accelerate, vulnerabilities such as CVE-2024-2371 underscore the critical importance of robust security measures tailored to the unique challenges of industrial environments. Proactive security practices, including regular risk assessments, timely patching, and effective intrusion detection, are imperative to safeguarding industrial control systems against evolving threats. By addressing CVE-2024-2371 and enhancing cybersecurity resilience, stakeholders can mitigate risks and ensure the integrity and reliability of industrial operations.

HADESS.IO

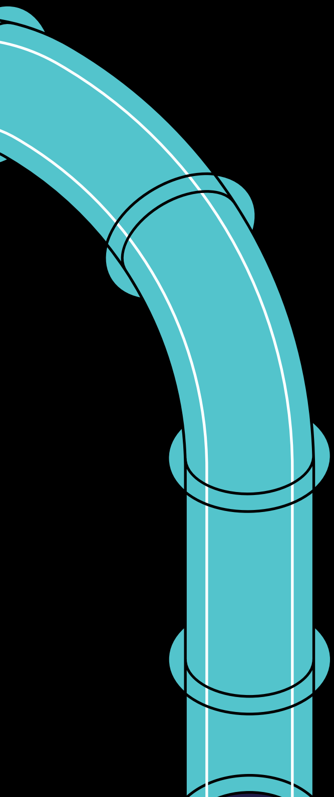
PLC I/O





01

Attacks



Attack Surface

Korenix JetBox is an industrial Ethernet switch designed for harsh environments and critical infrastructure applications. Here is an overview of its potential attack surface and security considerations:

- Web Interface - The switch can be managed through a web interface, which if not properly secured could allow an attacker to reconfigure the switch or exploit vulnerabilities in the web server. The web interface should be password protected and available only on management VLANs.

- SNMP - Simple Network Management Protocol is enabled by default and could let an attacker enumerate or reconfigure devices if the community strings are weak. SNMP should be disabled if not used or configured with least privilege access.

- Firmware - Bugs in the switch firmware could be exploited to take control of the system. The firmware should be kept up-to-date through Korenix security updates.

- Passwords - Weak or default passwords could let an attacker access the switch. Strong, unique passwords should be set for any switch user accounts.

- Network Access - The Ethernet ports on the switch could be an entry point into industrial networks. Use VLAN segmentation and access control lists to restrict traffic flows through the switch.

- Physical Access - Unrestricted physical access to the switch could let an attacker directly compromise it via the console port or by tampering. The switch should be physically secured and access audited.

Technical Analysis

Step1: Connect to the ICS network using a computer with appropriate permissions.
Open a command-line interface or terminal.

Step 2: Logging In
Assuming that the default credentials are "admin" for both username and password:

```
ssh admin@plc_device_ip
```

Replace plc_device_ip with the actual IP address of the PLC device.

Step 3: Listing Available I/O Modules
Once you've logged into the PLC, you might use a command to list the available I/O modules:

```
list-io-modules
```

Step 4: Configuring I/O Modules
Let's say you want to configure an analog input module:

```
configure-io-module --type analog-input --address 1 --range 4-20mA --scaling linear
```

Here, you're configuring an analog input module at address 1, specifying that it works with a 4-20mA range and uses linear scaling.

Step 5: Mapping I/O Points
You'll need to map physical I/O points to the configured module. For instance, map physical input 1 to the module address 1:

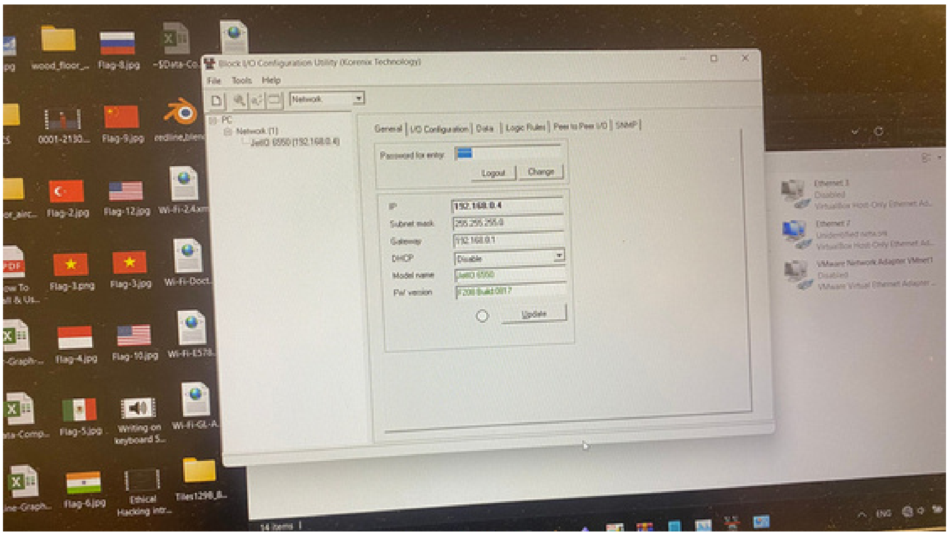
```
map-io-point --physical 1 --module-address 1 --module-point 1
```

Step 6: Saving Configuration
After configuring and mapping I/O points, it's important to save the configuration:

Step 7: Testing I/O
Now, you can test the I/O. Let's simulate a reading from input 1:

This command simulates a reading of 15.5 units from input 1.

Step 8: Monitoring
Monitor the I/O status for troubleshooting or ongoing operations:



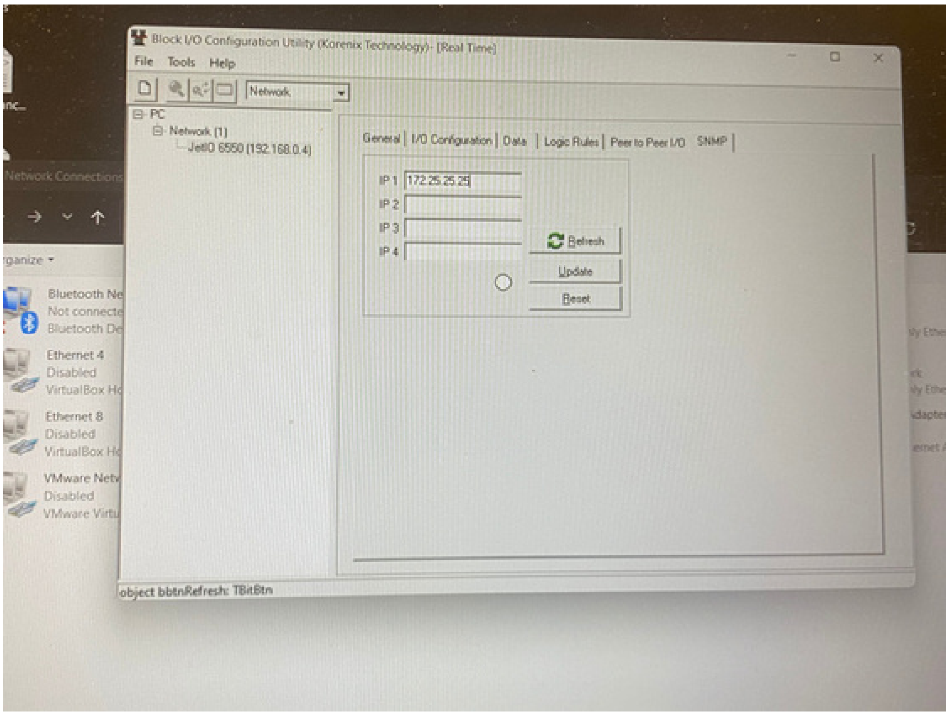
Block I/O Configuration Utility (Korenix Technology)

PC
Network (1)
JetIO 6550 (192.168.0.4)

General | I/O Configuration | Data | Logic Rules | Peer to Peer I/O | SNMP

Password for entry:

IP: 192.168.0.4
Subnet mask: 255.255.255.0
Gateway: 192.168.0.1
DHCP: Disable
Model name: JetIO 6550
F/W version: F208 Build 0817



Block I/O Configuration Utility (Korenix Technology)- [Real Time]

PC
Network (1)
JetIO 6550 (192.168.0.4)

General | I/O Configuration | Data | Logic Rules | Peer to Peer I/O | SNMP

IP 1: 172.25.25.25
IP 2:
IP 3:
IP 4:

object bbtnRefresh: TBitBtn

Configuring ICS I/O Devices Using SNMP

Step 1: Accessing the SNMP-Enabled I/O Device

- Connect to the ICS network using a computer with SNMP management capabilities.
- Open a command-line interface or terminal.

Step 2: Discovering SNMP Devices
Use an SNMP discovery tool to identify the SNMP-enabled I/O device on the network. For this example, let's assume the device has IP address 192.168.1.100:

```
snmpdiscover -t 192.168.1.100
```

Step 3: Accessing Device Information
Query the SNMP device for basic information. In this case, we'll query the system name and description:

```
snmpget -v2c -c admin 192.168.1.100 sysName.0 sysDescr.0
```

Step 4: Configuring I/O Modules
Assuming you've identified a specific OID (Object Identifier) for configuring I/O modules, you can use SNMP SET commands to configure them. Please note that real devices will have specific OIDs for various configuration parameters.

```
snmpset -v2c -c admin 192.168.1.100 <module_oid> <module_config_value>
```

Replace <module_oid> with the actual OID for module configuration and <module_config_value> with the desired configuration value.

Step 5: Mapping I/O Points
Assuming there's an OID for mapping I/O points, use SNMP SET to map physical I/O points to configured modules:

```
snmpset -v2c -c admin 192.168.1.100 <io_mapping_oid> <io_mapping_value>
```

Replace <io_mapping_oid> with the OID for I/O mapping and <io_mapping_value> with the desired mapping value.

Step 6: Testing I/O
To simulate a reading from an I/O point, use SNMP GET commands:

```
snmpget -v2c -c admin 192.168.1.100 <io_oid>
```

Replace <io_oid> with the OID of the I/O point you want to read.

Step 7: Monitoring I/O
You can continuously monitor I/O points using SNMP GET commands or by setting up SNMP traps for notifications:

```
snmpget -v2c -c admin 192.168.1.100 <io_oid>
```

Enabling Debug Mode in ICS I/O System

Identify the I/O System
Determine the specific I/O system you want to enable debug mode for. This could be a PLC, a SCADA system, or any other type of I/O system.

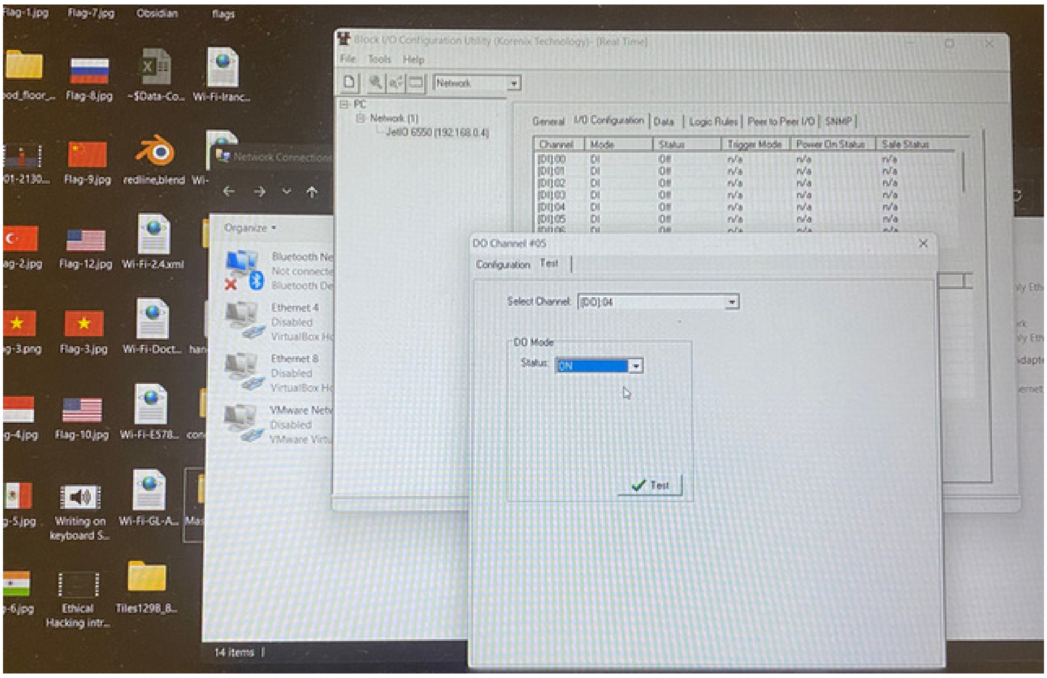
Enable Debug Mode
Within the configuration interface, you might have an option to enable debug mode. Let's assume the command to enable debug mode is as follows:

```
set-debug-mode --enable
```

Configure Debug Settings

Depending on the I/O system, you might also need to configure specific debug settings such as log levels, output destinations, or filters. These settings can help control the amount and type of debugging information that is generated.

In this example, you're setting the log level to "verbose" and specifying that the debug output should be saved to a file named "debug.log."



Channel	Mode	Status	Trigger Mode	Power On Status	Safe Status
[DI]:00	DI	Off	n/a	n/a	n/a
[DI]:01	DI	Off	n/a	n/a	n/a
[DI]:02	DI	Off	n/a	n/a	n/a
[DI]:03	DI	Off	n/a	n/a	n/a
[DI]:04	DI	Off	n/a	n/a	n/a
[DI]:05	DI	Off	n/a	n/a	n/a

Select Channel: [DO]:04

Status: ON

Logic Rule Condition and Writing Digital Data to a Relay

Create a Logic Rule

Assuming the logic configuration interface allows you to create rules, let's create a rule to control a relay based on a condition. For example, let's say you want to activate the relay when the temperature exceeds 80 degrees Celsius.

- Navigate to the "Rules" or "Logic" section of the interface.
- Create a new rule and name it "Temperature Control."
- Define the condition: IF Temperature > 80 THEN Activate Relay

Configure the Relay

Assuming the relay configuration section allows you to set the state of the relay, let's configure it to be controlled by the logic rule.

- Navigate to the "Relay Configuration" section.
- Locate the relay you want to control and assign it to the "Temperature Control" rule.

Save and Apply Configuration

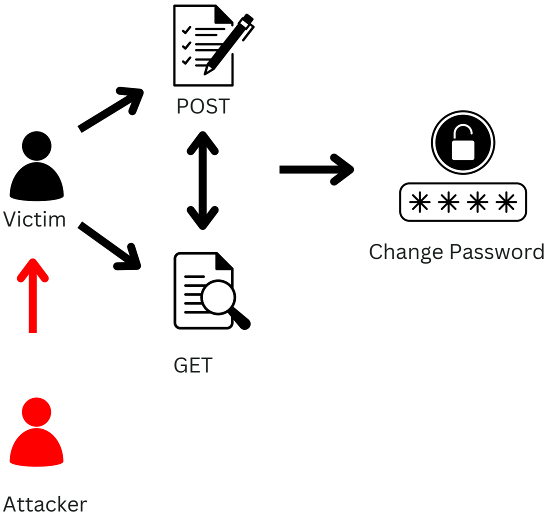
After setting up the logic rule and configuring the relay, save and apply the configuration changes:

- Save the logic rule configuration.
- Save the relay configuration.

Test the Logic Rule

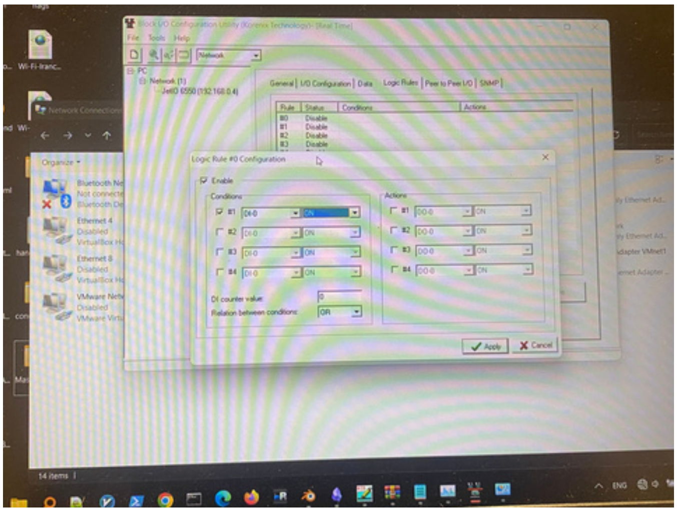
For testing purposes, simulate a temperature value exceeding 80 degrees Celsius to trigger the logic rule:

- Navigate to the "Simulation" or "Testing" section of the interface.
- Simulate a temperature value of 85 degrees Celsius.



Monitor the Relay State

Observe the relay state to confirm that it has been activated as a result of the logic rule condition:
Navigate to the "Relay Status" or "Monitoring" section.
Check the status of the relay assigned to the logic rule. It should be in the "Active" state.


Block I/O Configuration Utility (Korenix Technology) - [Real Time]

PC
Network (1)
JetIO 6550 (192.168.0.4)

General | I/O Configuration | Data | Logic Rules | Peer to Peer I/O | SNMP

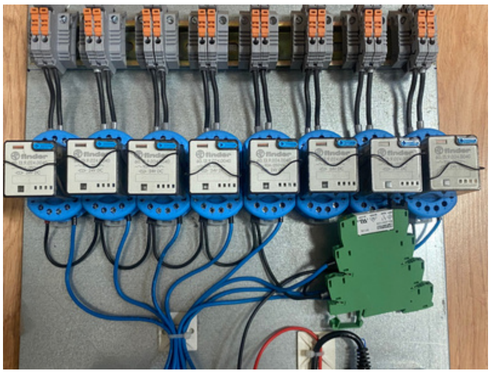
Rule	Status	Conditions	Actions
#0	Disable		
#1	Disable		
#2	Disable		
#3	Disable		

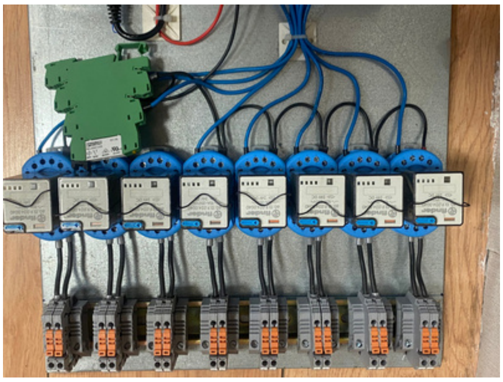
Logic Rule #0 Configuration

☑ Enable

Conditions
☑ #1 DI-0 ON
□ #2 DI-0 ON
□ #3 DI-0 ON
□ #4 DI-0 ON
DI counter value: 0
Relation between conditions: OR

Actions
□ #1 DO-0 ON
□ #2 DO-0 ON
□ #3 DO-0 ON
□ #4 DO-0 ON

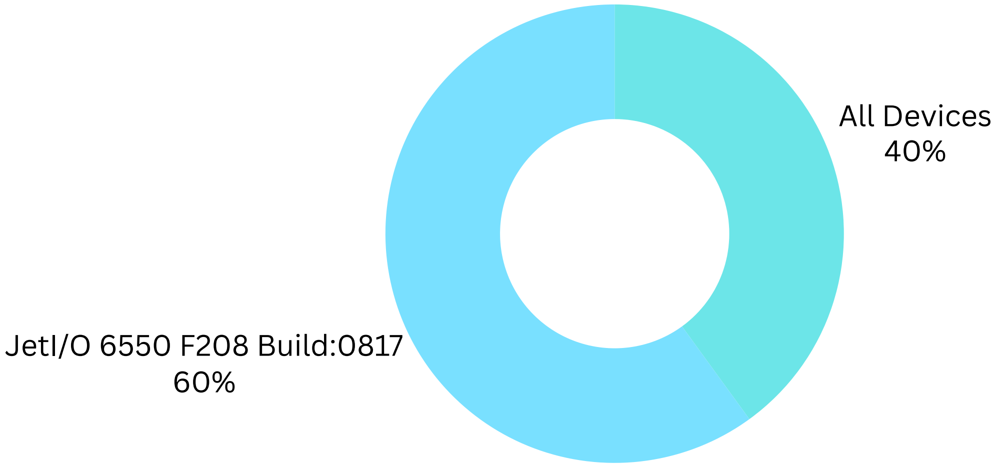


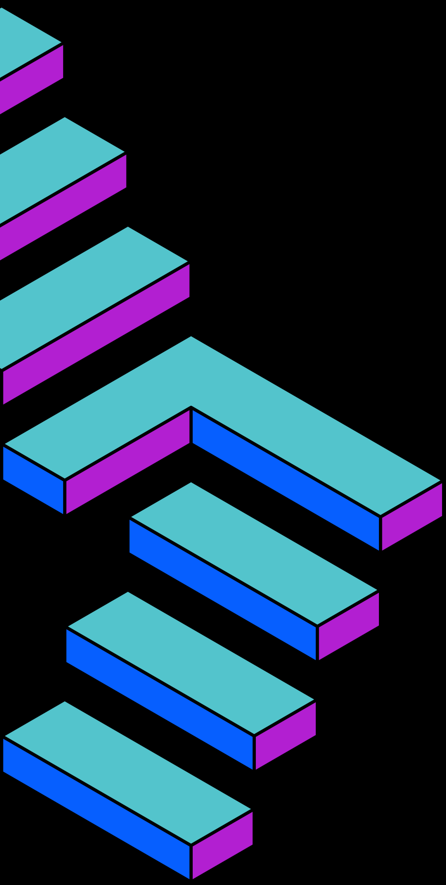


Scope of the Issues

The CVE-2024-2371 vulnerability in Korenix JetIO switches encompasses a broad spectrum of potential issues and impacts within industrial control systems (ICS) and critical infrastructure. At its core, this vulnerability exposes sensitive data to unauthorized access through the exploitation of the Simple Network Management Protocol (SNMP) implementation. The scope of the issues stemming from this vulnerability can be categorized into several key areas:

1. Data Exposure: The primary concern is the unauthorized access to sensitive data stored within Korenix JetIO switches. This includes configuration details, network topology information, and other critical parameters necessary for the operation of industrial systems. The exposure of such data can facilitate targeted attacks, operational disruptions, and compromises to system integrity.
2. Operational Disruptions: The exploitation of CVE-2024-2371 poses a significant risk of operational disruptions within industrial environments. Malicious actors could exploit the vulnerability to manipulate system settings, disrupt network communications, or cause equipment malfunctions. These disruptions can lead to downtime, production losses, and potential safety hazards.
3. Network Compromise: Given the interconnected nature of industrial networks, a successful exploit of the Korenix vulnerability can lead to broader network compromises. Attackers could leverage compromised Korenix JetIO switches as entry points to infiltrate other systems or spread malware within the network. This could result in the compromise of additional critical infrastructure components and exacerbate the overall impact of the attack.
4. Financial and Reputational Damage: The fallout from a CVE-2024-2371 exploitation extends beyond immediate operational disruptions. Industrial organizations may incur financial losses due to downtime, remediation efforts, and potential regulatory fines. Moreover, the reputational damage resulting from a security breach can erode trust among customers, investors, and stakeholders, leading to long-term consequences for the organization.
5. Safety Concerns: In certain industrial settings, such as manufacturing plants or utilities, the compromise of control systems due to CVE-2024-2371 exploitation can pose significant safety risks. Manipulation of operational parameters or equipment malfunctions resulting from unauthorized access can jeopardize the safety of personnel, assets, and the surrounding environment.





Conclusion

In conclusion, CVE-2024-2371 represents a significant security concern for industrial control systems utilizing Korenix JetIO switches. By exploiting weaknesses in SNMP, malicious actors can potentially compromise sensitive data and disrupt critical operations. Addressing this vulnerability demands proactive measures from both vendors and operators, emphasizing the importance of robust security practices tailored to the unique challenges of industrial environments.

HADESS

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

WWW.HADESS.IO

Email

MARKETING@HADESS.IO

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.