Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cracking Open the Dual Weaknesses of Rockwell Automation's PanelView Plus

Date of Publication	Admiralty Code	TA Number
July 8, 2024	A1	TA2024262

Summary

First Seen: July 2024
Affected Products: Rockwell Automation PanelView Plus
Impact: Two critical security flaws have been identified in Rockwell Automation's PanelView Plus. These vulnerabilities can be exploited by remote, unauthenticated attackers to execute arbitrary code or trigger a denial-of-service (DoS) condition. The successful exploitation of these flaws poses a significant threat, potentially leading to information disclosure or a DoS condition, which can severely impact the operational integrity and security of the affected systems.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-2071	FactoryTalk View Machine Edition Remote Code Execution Vulnerability	FactoryTalk View Machine Edition	✗	✗	✓
CVE-2023-29464	FactoryTalk Linx Denial-of-Service and Information Disclosure Vulnerability	FactoryTalk® Linx	✗	✗	✓

Vulnerability Details

#1 Rockwell Automation discovered two critical vulnerabilities in PanelView Plus devices, widely used in industrial sectors as graphic terminals. The first vulnerability allows remote code execution (RCE) through custom classes that load malicious DLL files. The second vulnerability causes denial-of-service (DoS) by exploiting buffer handling issues with crafted data packets.

#2 In FactoryTalk View Machine Edition on PanelView Plus, a CVE-2023-2071 flaw allows unauthenticated attackers to execute remote code via maliciously crafted packets. The vulnerability stems from Common Industrial Protocol (CIP) class that executes exported functions from libraries, with a routine intended to restrict it to specific functions from designated dll file. An attacker can circumvent this restriction by uploading a custom library, thereby bypassing security checks and exploiting the vulnerability.

#3 The CVE-2023-29464 flaw in FactoryTalk Linx on Rockwell Automation PanelView Plus permits unauthenticated threat actors to access memory data via malicious packets. By sending packets larger than the buffer size, attackers can leak data and disclose information. Large packets can also disrupt communications over the common industrial protocol, potentially leading to a DoS condition for FactoryTalk® Linx.

#4 Researchers identified two custom CIP classes within Rockwell's DLL that are vulnerable to exploitation through malicious uploads. One class is responsible for performing file read/write operations on the device, allowing attackers to upload a malicious DLL. The second class is tasked with loading the specified DLL, which they leveraged to execute the malicious DLL, gaining full control over the device. Notably, both classes have weak and permissive security checks.

#5 Successful exploitation of these vulnerabilities allows adversaries to execute remote code, potentially disclose information, or cause a DoS condition. It is crucial to apply patches to affected devices within your network, specifically targeting vulnerabilities in FactoryTalk View ME and FactoryTalk Linx on PanelView Plus. Start by identifying impacted devices and promptly installing the necessary patches.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-2071	FactoryTalk View Machine Edition: 12.0 - 13.0	cpe:2.3:a:rockwellautomation:factorytalk_view:*:*:*:*:machine:*:*:* cpe:2.3:h:rockwellautomation:panelview_plus:-:*:*:*:*:*:*:*	CWE-20
CVE-2023-29464	FactoryTalk Linx: 6.20	cpe:2.3:a:rockwellautomation:factorytalk_linx:6.20:*:*:*:*:*:*:* cpe:2.3:a:rockwellautomation:factorytalk_linx:6.30:*:*:*:*:*:*:*	CWE-20

Recommendations

Update: To mitigate the risk posed by CVE-2023-2071 and CVE-2023-29464, update FactoryTalk View Machine Edition and FactoryTalk Linx to the latest version, which addresses the vulnerability. Users are strongly advised to update to this version to reduce the risk of exploitation.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0005** Defense Evasion	**TA0040** Impact
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1498** Network Denial of Service
T1129 Shared Modules	**T1112** Modify Registry	**T1574** Hijack Execution Flow	**T1574.011** Services Registry Permissions Weakness

Patch Details

To mitigate the risks posed by CVE-2023-2071 and CVE-2023-29464, it is crucial to update FactoryTalk View Machine Edition and FactoryTalk Linx to their latest versions, which have been patched to address these vulnerabilities. Users are strongly advised to perform these updates promptly to minimize the risk of exploitation.

Links:
https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1645%20.html

https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1652.html

References

https://www.microsoft.com/en-us/security/blog/2024/07/02/vulnerabilities-in-panelview-plus-devices-could-lead-to-remote-code-execution/

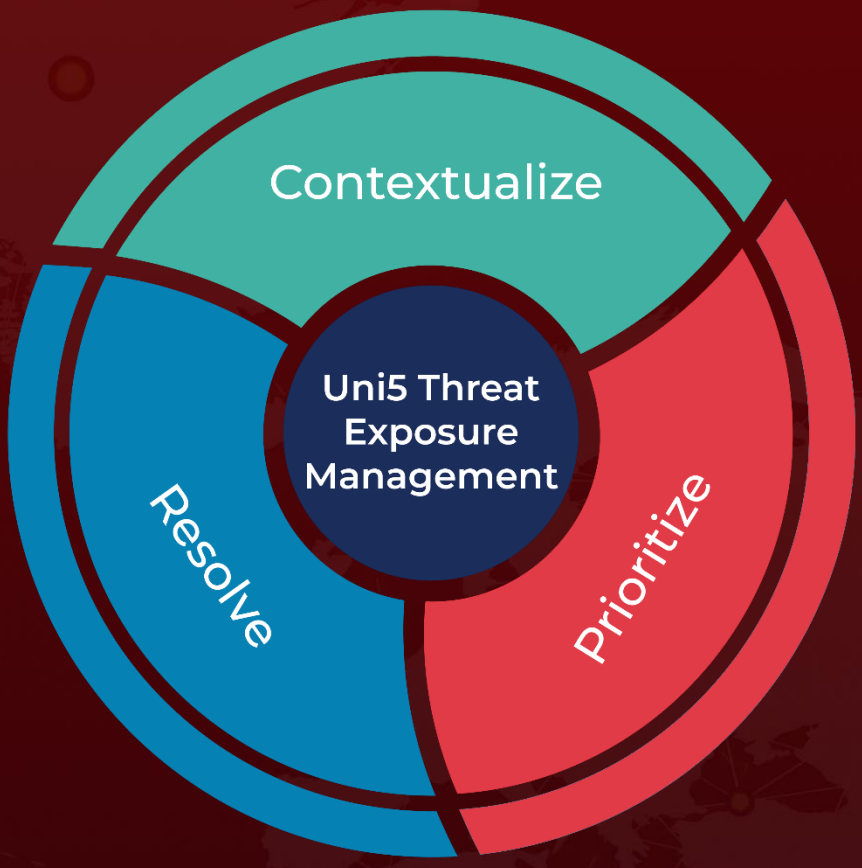
https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1645%20.html

https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1652.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 8, 2024 • 7:30 AM

More at www.hivepro.com