Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Rust Flaw Renders Windows Systems Vulnerable

Date of Publication	Admiralty Code	TA Number
April 10, 2024	A1	TA2024137

Summary

Discovered: April 2024
Affected Products: Rust standard library
Impact: The critical security vulnerability CVE-2024-24576 affects the Rust standard library and poses a significant risk to Windows users. This flaw can be exploited to conduct command injection attacks, leveraging weaknesses related to OS command and argument handling.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-24576	Rust Arbitrary Shell Command Vulnerability	Rust library	✗	✗	✓

Vulnerability Details

#1 The vulnerability identified as CVE-2024-24576 poses a significant threat as threat actors can exploit it to launch command injection attacks on Windows systems. This flaw arises from weaknesses in handling OS commands and arguments within the Rust standard library. Attackers could leverage this vulnerability to execute unexpected and potentially malicious commands on the targeted operating system, leading to severe security breaches and system compromises.

#2 The flaw stems from the Rust standard library's Command API failing to properly escape parameters when invoking batch files (with the bat and cmd extensions) on Windows. As a result, attackers could bypass this escaping mechanism, allowing them to execute arbitrary shell commands by manipulating the inputs provided to the generated process.

#3 The library implemented specialized escape mechanisms for command arguments in batch files. However, a flaw was discovered in the escape logic, rendering it inadequate and potentially allowing the execution of malicious inputs. This vulnerability poses a severe risk, especially when untrusted arguments are used to invoke batch files on Windows systems. It's important to note that this vulnerability does not affect other platforms or use cases.

#4 To address the challenge posed by the complexity of cmd.exe, the Rust made changes to the Command API to enhance the resilience of the escape code. As part of these improvements, the API now generates an InvalidInput error if it encounters difficulties securely escaping an argument. Additionally, the CommandExt::raw_arg method serves as a workaround specifically designed for Windows systems, providing an alternative to the standard library's escape logic.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-24576	All Rust versions before 1.77.2 on Windows	cpe:2.3:a:rust:rust:1.77.0:*:*:*:*:*:*:* cpe:2.3:a:rust:rust:1.77.1:*:*:*:*:*:*:*	CWE-88

Recommendations

- **Keep Libraries Updated:** Ensure that all libraries are regularly updated to the latest versions to patch known vulnerabilities.
- **Deploy Behavioral Analysis Solutions:** Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.
- **Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent threats from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0005 Defense Evasion	T1202 Indirect Command Execution
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	

Patch Details

To update Rust to the latest version (1.77.2) and address the CVE-2024-24576 flaw, you can use the following command 'rustup update stable'.

To install you can visit the official Rust website and follow the provided instructions.

Link: https://www.rust-lang.org/tools/install

References

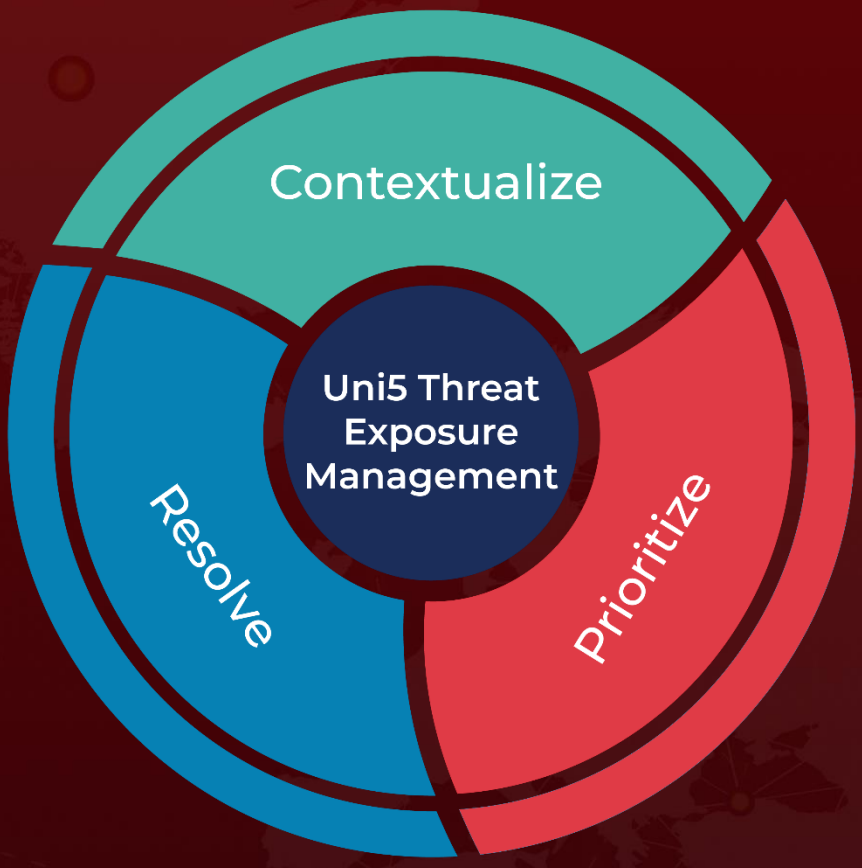
https://blog.rust-lang.org/2024/04/09/cve-2024-24576.html

https://blog.rust-lang.org/2024/04/09/Rust-1.77.2.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

April 10, 2024 • 5:30 AM

More at www.hivepro.com