CERT-EU

Security Advisory 2024-035

Critical Vulnerability in Rust on Windows

April 10, 2024 — v1.0

TLP:CLEAR

History:

- *10/04/2024 — v1.0 – Initial publication*

Summary

On April 9, 2024, the Rust Security Response WG issued a security advisory regarding a critical vulnerability in the Rust programming environment affecting Windows platforms. This flaw allows command injection attacks via crafted batch file executions with untrusted arguments.

It is recommended updating as soon as possible, prioritising assets running code (or one of its dependencies) which executes batch files with untrusted arguments [1].

Technical Details

The vulnerability, identified as **CVE-2024-24576** with a CVSS score of 10, stems from improper sanitisation of command-line arguments which could be manipulated to execute arbitrary commands. This issue affects all Rust versions prior to 1.77.2 on Windows if a program's code or one of its dependencies invokes and executes batch files with untrusted arguments [1].

Affected Products

All Rust versions before 1.77.2 on Windows are affected [2].

Recommendations

CERT-EU recommends upgrading Rust prioritising assets running code (or one of its dependencies) which executes batch files with untrusted arguments.

References

[1] https://www.bleepingcomputer.com/news/security/critical-rust-flaw-enables-windows-command-injection-attacks/

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