April 8, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Red Hat published security advisories to address vulnerabilities in multiple products. Included were updates to address vulnerabilities in the Linux kernel for the following products:

- Red Hat CodeReady Linux Builder – multiple versions and platforms
- Red Hat Enterprise Linux – multiple versions and platforms
- Red Hat Enterprise Linux Server – multiple versions and platforms
- Red Hat Virtualization Host – multiple versions and platforms

Technical Details
Security Fix(es):

- argo-cd: Denial of Service Due to Unsafe Array Modification in Multi-threaded Environment (CVE-2024-21661)
- argo-cd: Users with `create` but not `override` privileges can perform local sync (CVE-2023-50726)
- argo-cd: Bypassing Brute Force Protection via Application Crash and In-Memory Data Loss (CVE-2024-21652)
- argo-cd: uncontrolled resource consumption vulnerability (CVE-2024-29893)
- argo-cd: Bypassing Rate Limit and Brute Force Protection Using Cache Overflow(CVE-2024-21662)

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-29893 CVE-2024-21662 CVE-2024-21661 CVE-2024-21652 CVE-2024-0553 CVE-2023-52425 CVE-2023-50726
- Red Hat Security Advisories