July 10, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of 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 Server – multiple versions and platforms Red Hat Enterprise Linux – multiple versions and platforms Red Hat Enterprise Linux for Real Time – multiple versions and platforms

Technical Details

A signal handler race condition vulnerability was found in OpenSSH's server (sshd) in Red Hat Enterprise Linux 9, where a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then sshd's SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog(). This issue leaves it vulnerable to a signal handler race condition on the cleanup_exit() function, which introduces the same vulnerability as CVE-2024-6387 in the unprivileged child of the SSHD server. As a consequence of a successful attack, in the worst case scenario, the attacker may be able to perform a remote code execution (RCE) within unprivileged user running the sshd server. This vulnerability affects only the sshd server shipped with Red Hat Enterprise Linux 9, while upstream versions of sshd are not impact by this flaw.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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 VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2024-33871 CVE-2024-26585 CVE-2024-6387 CVE-2024-6409
- Red Hat Security Advisory – RHSA-2024:4352
- Red Hat Security Advisory – RHSA-2024:4349
- Red Hat Security Advisory – RHSA-2024:4211
- Red Hat Security Advisories