August 6, 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 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 Enterprise Linux – multiple versions and platforms
- Red Hat Enterprise Linux Server – multiple versions and platforms
- Red Hat Enterprise Linux for Real Time – multiple versions and platforms
- Red Hat CodeReady Linux Builder – multiple versions and platforms

Technical Details

A flaw was found in the package index module of pypa/setuptools. Affected versions of this package allow remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system.

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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-6345 CVE-2024-38473 CVE-2024-39573 CVE-2024-38428
- Red Hat Security Advisories