RHSA-2025:22660 - Security Advisory

发布： 2025-12-03 已更新： 2025-12-03

概述

更新的软件包

概述

Moderate: systemd security update

类型/严重性

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

查看受影响的系统

标题

An update for systemd is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

描述

The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount points, and implements an elaborate transactional dependency-based service control logic. It can also work as a drop-in replacement for sysvinit.

Security Fix(es):

- systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain read access to the resulting core dump (CVE-2025-4598)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

解决方案

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

受影响的产品

- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64

修复

- BZ - 2369242 - CVE-2025-4598 systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain read access to the resulting core dump

CVE

- CVE-2025-4598

参考

- https://access.redhat.com/security/updates/classification/#moderate

Red Hat 安全团队联络方式为 secalert@redhat.com。 更多联络细节请参考 https://access.redhat.com/security/team/contact/。