RHSA-2023:5455 - Security Advisory

Issued: 2023-10-05 Updated: 2023-10-05

Synopsis

Important: glibc security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for glibc is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Important. 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.

Description

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Security Fix(es):

- glibc: buffer overflow in ld.so leading to privilege escalation (CVE-2023-4911)
- glibc: Stack read overflow in getaddrinfo in no-aaaa mode (CVE-2023-4527)
- glibc: potential use-after-free in getaddrinfo() (CVE-2023-4806)
- glibc: potential use-after-free in gaih_inet() (CVE-2023-4813)

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.

Solution

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

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

For the update to take effect, all services linked to the glibc library must be restarted, or the system rebooted.

Affected Products

- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.8 x86_64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
- Red Hat CodeReady Linux Builder for x86_64 8 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64

- Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.8 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64

Fixes

- BZ - 2234712 - CVE-2023-4527 glibc: Stack read overflow in getaddrinfo in no-aaaa mode
- BZ - 2237782 - CVE-2023-4806 glibc: potential use-after-free in getaddrinfo()
- BZ - 2237798 - CVE-2023-4813 glibc: potential use-after-free in gaih_inet()
- BZ - 2238352 - CVE-2023-4911 glibc: buffer overflow in ld.so leading to privilege escalation

CVEs

- CVE-2023-4527
- CVE-2023-4806
- CVE-2023-4813
- CVE-2023-4911

References

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

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.