CVE Security Report

CVE: CVE-2016-2781

Description: chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.

Impact Score: Not Available

References:

http://www.openwall.com/lists/oss-security/2016/02/28/2
http://www.openwall.com/lists/oss-security/2016/02/28/3
https://lists.apache.org/thread.html/rf9fa47ab66495c78bb4120b0754dd9531ca2ff0430
f6685ac9b07772%40%3Cdev.mina.apache.org%3E http://www.openwall.com/lists/oss-security/2016/02/28/2
http://www.openwall.com/lists/oss-security/2016/02/28/3
https://lists.apache.org/thread.html/rf9fa47ab66495c78bb4120b0754dd9531ca2ff0430
f6685ac9b07772%40%3Cdev.mina.apache.org%3E

CVE: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.

Impact Score: 3.3

References:

https://access.redhat.com/security/cve/CVE-2022-3219 https://bugzilla.redhat.com/show_bug.cgi?id=2127010
https://dev.gnupg.org/D556 https://dev.gnupg.org/T5993
https://marc.info/?l=oss-security&m;=165696590211434&w;=4
https://security.netapp.com/advisory/ntap-20230324-0001/
https://access.redhat.com/security/cve/CVE-2022-3219 https://bugzilla.redhat.com/show_bug.cgi?id=2127010
https://dev.gnupg.org/D556 https://dev.gnupg.org/T5993
https://marc.info/?l=oss-security&m;=165696590211434&w;=4
https://security.netapp.com/advisory/ntap-20230324-0001/

HIGH RISK

CVE: CVE-2025-0395

Description: When the assert() function in the GNU C Library versions 2.13 to 2.40 fails, it does not allocate enough space for the assertion failure message string and size information, which may lead to a buffer overflow if the message string size aligns to page size.

Impact Score: 7.5

References:

https://sourceware.org/bugzilla/show_bug.cgi?id=32582
https://sourceware.org/git/?p=glibc.git;a=blob;f=advisories/GLIBC-SA-2025-0001
https://sourceware.org/pipermail/libc-announce/2025/000044.html
https://www.openwall.com/lists/oss-security/2025/01/22/4
http://www.openwall.com/lists/oss-security/2025/01/22/4
http://www.openwall.com/lists/oss-security/2025/01/23/2
https://security.netapp.com/advisory/ntap-20250228-0006/

HIGH RISK

CVE: CVE-2016-20013

Description: sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algorithm's runtime is proportional to the square of the length of the password.

Impact Score: 7.5

References:

https://akkadia.org/drepper/SHA-crypt.txt
https://pthree.org/2018/05/23/do-not-use-sha256crypt-sha512crypt-theyre- dangerous/
https://twitter.com/solardiz/status/795601240151457793 https://akkadia.org/drepper/SHA-crypt.txt
https://pthree.org/2018/05/23/do-not-use-sha256crypt-sha512crypt-theyre- dangerous/
https://twitter.com/solardiz/status/795601240151457793

HIGH RISK

CVE: CVE-2025-0395

Description: When the assert() function in the GNU C Library versions 2.13 to 2.40 fails, it does not allocate enough space for the assertion failure message string and size information, which may lead to a buffer overflow if the message string size aligns to page size.

Impact Score: 7.5

References:

https://sourceware.org/bugzilla/show_bug.cgi?id=32582
https://sourceware.org/git/?p=glibc.git;a=blob;f=advisories/GLIBC-SA-2025-0001
https://sourceware.org/pipermail/libc-announce/2025/000044.html
https://www.openwall.com/lists/oss-security/2025/01/22/4
http://www.openwall.com/lists/oss-security/2025/01/22/4
http://www.openwall.com/lists/oss-security/2025/01/23/2
https://security.netapp.com/advisory/ntap-20250228-0006/

CVE: CVE-2016-20013

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2025-1390

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-2236

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-12243

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10041

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10963

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10041

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10963

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10041

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10963

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10041

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-10963

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-13176

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-41996

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-9143

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-12133

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-56433

Description: Error fetching data

Impact Score: Not Available

References:

None

CVE: CVE-2024-56433

Description: Error fetching data

Impact Score: Not Available

References:

None