



Security

[Get Gentoo!](#)

[gentoo.org sites](#)

[gentoo.org Wiki](#) [Bugs](#) [Forums](#) [Packages](#)

[Planet](#) [Archives](#) [Sources](#)

[Infra Status](#)

□

- [Home](#)
- [Stay informed](#)
- [Advisories](#)

xterm: Arbitrary Code Execution — GLSA 202211-09

A vulnerability has been found in xterm which could allow for arbitrary code execution.

Affected packages

Package x11-terms/xterm on all architectures

Affected versions < 375

Unaffected versions >= 375

Background

xterm is a terminal emulator for the X Window system.

Description

xterm does not correctly handle control characters related to OSC 50 font ops sequence handling.

Impact

The vulnerability allows text written to the terminal to write text to the terminal's command line. If the terminal's shell is zsh running with vi line editing mode, text written to the terminal can also trigger the execution of arbitrary commands via writing ^G to the terminal.

Workaround

As a workaround, users can disable xterm's usage of OSC 50 sequences by adding the following to the XResources configuration: `XTerm*allowFontOps: false`

Resolution

All xterm users should upgrade to the latest version:

```
# emerge --sync  
# emerge --ask --oneshot --verbose ">=x11-terms/xterm-375"
```

References

- [CVE-2022-45063](#)

Release date

November 22, 2022

Latest revision

November 22, 2022: 1

Severity

normal

Exploitable

remote

Bugzilla entries

- [880747](#)

Questions or comments?

Please feel free to [contact us](#).

-
-

© 2001–2026 Gentoo Foundation, Inc.

Gentoo is a trademark of the Gentoo Foundation, Inc. The contents of this document, unless otherwise expressly stated, are licensed under the [CC-BY-SA-4.0](#) license. The [Gentoo name and logo usage guidelines](#) apply.