

Xerus Firmware Release Notes



Version: Xerus 4.4.1 / Build 53217

Release Status: Limited Availability (LA)

Date: October 12, 2026

Xerus 4.4.1 Firmware is a LA Release. It may include performance and productivity improvements, support for new products and accessories, new features and enhancements, bug fixes, and general fixes for specific model families.

Applicability

This firmware release applies to the following product groups and models:

Product Group	Model
Server Technology® Rack PDUs	PRO4X

This firmware release does not support Server Technology PRO1, PRO2, Sentry CDU, EMCU, EMTH, or EMWS models.

Upgrade Path

This firmware release is intended for factory shipments and firmware upgrades for the units/models listed in the Applicability table above. If you are unsure of your unit's model number, you can typically find it on the GUI's Device Information page and on a label on the device. (This release may not support some custom-engineered models.)

The release package for this firmware update is available at servertech.com/support/rack-pdu-firmware-downloads.

Because of file system changes in Xerus 4.0.x, follow the upgrade paths below, or the device may become inoperable and require manual recovery.

If the Applicable Device's Current Firmware Version Is...	Follow These Upgrade Steps
Xerus 4.0.x, 4.1.x	» 4.2.0 » 4.4.1
Xerus 4.2.x, 4.3.x, 4.4.0	» 4.4.1

Note: Do NOT downgrade your new Xerus-based product(s) to any prior Xerus Firmware release. A downgrade to ANY prior firmware release is NOT SUPPORTED.

Release Highlights

Bug Fixes

Issue ID	Description
89857	Addressed potential text parsing issue for open source package versions
89484	Addressed potential source of Crestron daemon segfaults

Security Updates

Issue ID	Description
89750	Upgraded Linux kernel to address a number of Linux kernel CVEs
89540	Addresses potential out-of-bounds element ID reads (CVE-2026-68402)
89536	Addresses potential issue with ACK validation (CVE-2026-68118)
89534	Addresses potential source of Linux kernel panics (CVE-2026-68136)
89474	Addresses potential issue allowing crafted packets to prematurely drop active connections (CVE-2026-63913)
89476	Addresses potential memory handling flaw in IPv6 packet handling (CVE-2026-64554)
89222	Addresses potential memory corruption in Linux kernel IPv6 multicast handling that could allow denial of service or code execution (CVE-2026-53275)
89176	Addresses potential Linux kernel panic when processing certain network traffic (CVE-2026-53235)
89640 89623 89589	Addresses vulnerabilities across various services that could allow administrator users to execute root shell commands

Contact Us

Go to servertech.com/support for contact options.