

Xerus Firmware Release Notes



Version: Xerus 4.3.14 / Build 52917

Release Status: General Availability (GA)

Date: July 17, 2026

Xerus 4.3.14 Firmware is a GA Release and 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
Raritan® Rack PDUs	PX3, PX2, PXC, PXO
Raritan Inline Meters	PX3
Raritan Rack Transfer Switches	PX3TS
Raritan Branch Circuit Monitors	BCM2
Raritan Smart Rack Controllers	SRC

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, it is typically visible on the Device Information page of the GUI and also printed 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 raritan.com/support/product/pdu-g2.

Due to file system changes in Xerus 4.0.x, the following upgrade paths must be followed, or the Xerus-based device may become inoperable and require manual recovery.

If the Applicable Device's Current Firmware Version Is...	Follow These Upgrade Steps
Xerus 3.0.x, 3.1.x, 3.2.x	» 3.4.0 » 3.5.0 » 4.3.14
Xerus 3.3.x, 3.4.x	» 3.5.0 » 4.3.14
Xerus 3.5.x, 3.6.x	» 4.3.14
Xerus 4.0.x	» 4.3.14
Xerus 4.1.x, 4.2.x, 4.3.x	» 4.3.14

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

Security Fixes & Updates

Issue ID	Description
88951	Critical fix for privilege escalation issue with SCP
89000	Addressed Remote exploitable vulnerability IPv6 (CVE-2026-43501)
89003	Addressed Remote exploitable vulnerability ICMP (CVE-2026-46037)
89004	Updated OpenSSL to version 3.0.21 for firmware versions 4.3.x
89171	Addressed LAN-exploitable vulnerability IPv6 (CVE-2026-53275)

Contact Us

Go to raritan.com/support for contact options.