(https://keenetic.com/global)

Keenetic Product Security Advisory

ENG

Ensuring our customers' protection against security threats is Keenetic's highest priority. We design innovative products and services from the ground up, with a strong commitment to reliability, security, and user privacy.

We encourage and welcome reports concerning product security or privacy issues. For any security-related inquiries or to report vulnerabilities, please contact the Keenetic Security Team at security@keenetic.com (mailto:security@keenetic.com).

Security Center

Keenetic Coordinated Vulnerability Disclosure Policy

Keenetic - Bug Bounty Terms & Conditions

Anonymous Vulnerability Disclosure Form (https://keenetic.com/global/security/anonymous-reporting-form?lang=en)

Security Updates

> **Statement on Privilege Escalation from Read-Only User to Administrator (pre-KeeneticOS 5.0)**

Statement on the Issue of Weak Passwords Allowed for Remote Web Access (pre-KeeneticOS 4.3)

Statement on Web API Vulnerabilities Prior to KeeneticOS 4.3

(https://keenetic.com/global)

Statement on Mobile App Database Unauthorized Access

Statement on Information Disclosure Vulnerabilities CVE-2024-4021 and CVE-2024-4022

Statement on FragAttacks Vulnerabilities

Statement on Privilege Escalation from Read-Only User to Administrator (pre-KeeneticOS 5.0)

Last update 27-01-2026

Advisory ID: KEN-PSA-2026-WP01
Severity: High
Status: Resolved in KeeneticOS 5.0.4 and later

Summary

A security issue has been identified in KeeneticOS that allows a user with read-only access to extract internal system information and leverage it to elevate privileges to an administrator level. This issue requires prior authenticated access as a read-only user, but can be exploited remotely.

Affected Products / Configurations

Products: Keenetic routers running versions of KeeneticOS earlier than 5.0.4.

Configuration prerequisite: The attacker must already possess valid read-only credentials on the device's management interface.

Vulnerability Details

The vulnerability stems from insufficient isolation of sensitive configuration data accessible to read-only accounts. A user authenticated with read-only privileges can retrieve specific internal parameters from the device. When combined, these parameters enable the attacker to escalate their privileges and gain administrative access to the router's management interface.

(https://keenetic.com/global)

CVSS (High) — AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Rationale: The attack requires only low-privilege authenticated access, is remotely exploitable, and results in full compromise of confidentiality, integrity, and availability.

Remediation & Hardening

Upgrade: Transfer all devices running versions earlier than 5.0 to KeeneticOS 5.0.4 or later. Use the latest OS available for your model.

Interim mitigation: Avoid creating or assigning read-only user accounts until the update is applied.

© Keenetic Limited 2010–2026