Security Bulletin

Bulletin ID: RITTAL-SA-C-2026-0004
Project: RITTAL ReOS1 - IOT
Version: v10.1.3
Compared against: v10.1.2
Generated on: 13.05.2026
Classification: TLP:CLEAR

Summary

This bulletin documents 1 security vulnerabilities (1 High) that were fixed in RITTAL ReOS1 - IOT version v10.1.3 compared to version v10.1.2. Rittal recommends updating to the latest firmware version.

Table of Contents

Affected Products (Article Numbers)

Article Number	Description
3312.800	Bundle Blue e+ IT, SK Dachaufbau-Kühlgerät 1,6 kW, RAL 7035
3312.810	Blue e+ für IT, SK Wandkühlgerät 3 kW mit IoT Interface, BHT: 450x1600x294 mm
3399.022	N/A
3412.800	Bundle Blue e+ IT, SK Dachaufbau-Kühlgerät 1,6 kW, R-1234yf
3412.810	Blue e+ für IT, SK Wandkühlgerät 3 kW mit IoT Interface, R-1234yf

Fixed Vulnerabilities Overview

All	Critical	High	Medium	Low
1	0	1	0	0

Fixed Vulnerabilities

CVE	Severity	CVSS	CVSS Vector	Component	Description
CVE-2025-15467	HIGH	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	openssl 3.2.6	Issue summary: Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. When parsing CMS (Auth)EnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Applications and services that parse untrusted CMS or PKCS#7 content using AEAD ciphers (e.g., S/MIME (Auth)EnvelopedData with AES-GCM) are vulnerable. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3 and 3.0 are vulnerable to this issue. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

Recommended Actions

Rittal recommends updating affected devices to firmware version **v10.1.3** or later to address the vulnerabilities listed in this bulletin.

Contact

For questions regarding this bulletin, please contact:
Rittal PSIRT – psirt@rittal.com

Disclaimer