Security Bulletin

Bulletin ID: RITTAL-SA-C-2026-0003
Project: RITTAL ReOS1 - CIOC1
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 - CIOC1 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
1182.140	N/A
1182.141	N/A
1182.143	N/A
3313.610	Liquid Cooling Unit LCU CW, L24/W15: 7,9 kW
3314.020	SK Aktivmodul für LCP RD CW, für Höhe =2000 mm, RAL 9005 Feinstruktur matt
3314.025	SK Aktivmodul für LCP RD CW, für Höhe =2200 mm, RAL 9005 Feinstruktur matt
3314.130	LCP Rack CW, 30 kW, RAL 7035, BHT: 300x2000x1000 mm
3314.230	LCP Rack CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.238	SK LCP Rack CW, 30 kW, UL
3314.250	LCP Rack CWG, 44 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.260	LCP Rack CW, 53 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.268	SK LCP Rack CW, 53 kW, UL
3314.530	LCP Inline CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.538	SK LCP Inline CW vorgezogen, 30 kW, UL
3314.540	LCP Inline CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.542	LCP Inline CW, 30 kW, RAL 7035, BHT: 300x2200x1200 mm
3314.548	SK LCP Inline CW bündig, 30 kW, UL
3314.550	LCP Inline CWG, 35 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.560	LCP Inline CW, 53 kW, RAL 7035, BHT: 300x2000x1200 mm
3314.568	SK LCP Inline CW vorgezogen, 53 kW, UL
3314.570	LCP Inline CWG, 44 kW, RAL 7035, BHT: 300x2000x1200 mm
3343.200	CDU In-Row, 1000 kW bei 4K ATD
3343.230	CDU In-Rack, 150 kW bei 6K ATD
3343.500	N/A
3343.620	N/A

Article Number	Description
3343.800	N/A
3396.813	N/A
3398.653	N/A
3399.100	N/A
7993.582	N/A

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