Security Bulletin

Bulletin ID: RITTAL-SA-I-2026-0003
Project: RITTAL ReOS1 - CMC3
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 - CMC3 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
3311.130	Luft/Wasser Wärmetauscher, Rackklimatisierung, T=1000 mm, 30 kW
3311.230	Luft/Wasser Wärmetauscher, Rackklimatisierung, T=1200 mm, 30 kW
3311.260	Luft/Wasser Wärmetauscher, Rackklimatisierung, T=1200 mm, 60 kW
3311.530	Luft/Wasser Wärmetauscher, Reihenklimatisierung, vorgezogen, 30 kW
3311.540	Luft/Wasser Wärmetauscher, Reihenklimatisierung, bündig mit Serverracks, 30 kW
3311.560	Luft/Wasser Wärmetauscher, Reihenklimatisierung, vorgezogen, 60 kW
3311.701	N/A
3311.702	N/A
3311.703	N/A
3311.704	N/A
3312.130	LCP Rack R15 CW, 30 kW, RAL 7035, BHT: 300x2000x1000 mm
3312.230	LCP Rack R15 CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.250	LCP Rack R15 CW/Glykol, 35 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.260	LCP Rack R15 CW, 55 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.530	LCP Inline Protruding R15 CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.540	LCP Inline Flush R15 CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.550	LCP Inline Flush R15 CW/Glykol, 35 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.560	LCP Inline Protruding R15 CW, 55 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.570	LCP Inline Protruding R15 CW/Glykol, 35 kW, RAL 7035, BHT: 300x2000x1200 mm
3312.701	N/A
3312.702	N/A
3312.703	N/A
3312.704	N/A
3313.130	LCP Rack CW, 30 kW, RAL 7035, BHT: 300x2000x1000 mm
3313.230	LCP Rack CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm

Article Number	Description
3313.238	SK LCP Rack CW UL, 30kW, RAL 9005, 300x2000x1200
3313.250	LCP Rack CWG, 44 kW, RAL 7035, BHT: 300x2000x1200 mm
3313.260	LCP Rack CW, 53 kW, RAL 7035, BHT: 300x2000x1200 mm
3313.268	SK LCP Rack CW UL, 53kW, 300x2000x1200, RAL 9005
3313.530	LCP Inline CW, 30 kW, RAL 7035, BHT: 300x2000x1200 mm
3313.538	SK LCP Inline CW UL, vorgezogen, 30kW, 300x2000x1200, RAL 9005
3313.540	N/A
3313.542	N/A
3313.548	SK LCP Inline CW UL, bündig, 30kW, 300x2000x1200, RAL 9005
3313.550	LCP Inline CWG, 35 kW, RAL 7035, BHT: 300x2000x1200 mm
3313.560	LCP Inline CW, 53 kW, RAL 7035, BHT: 300x2000x1200 mm
3313.568	SK LCP Inline CW UL vorgezogen, 53kW UL, 300x2000x1200, RAL 9005
3313.570	LCP Inline CWG, 44 kW, RAL 7035, BHT: 300x2000x1200 mm
3396.789	N/A
3396.795	N/A
3398.195	Steuermodul für LCP
3398.610	N/A
3398.611	N/A
7994.841	N/A
7994.843	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