KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “PHP Remote Code Execution PHP2Shell, October 2026” (KSA-2026-1)

In October 2026, new versions of PHP were released to address two remote code execution vulnerabilities tracked collectively as PHP2Shell. An unauthenticated, remote attacker could exploit these vulnerabilities to allow remote code execution.

For the affected products and services, Krones rates the likelihood of being exploited as medium. Therefore, timely action is recommended.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Medium	• Complete Steinecker BOTEC F1 process control systems with physical QNAP TS-435XeU NAS (QTS 5.2.11 and earlier)	• By default, the QNAP NAS is only accessible within the BOTEC F1 PCS OT network. Krones strongly recommends keeping the NAS isolated, only accessible to this network. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
Krones advises regularly reviewing its Security Advisories for updates. Subscribe to Krones Security Advisories at Security Advisories - Krones.			

Security contact

For any inquiries related to this Krones Security Advisory, please contact the Krones Product Security Incident Response Team (PSIRT) at cyber.security@krones.com. To communicate confidentially, you may use our OpenPGP key, available here: krones.com/ext/securitytxt/cyber.security@krones.com.asc

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Technical description of the security vulnerabilities

This section outlines security vulnerabilities addressed by this Krones Security Advisory. For each vulnerability, or grouped identical vulnerabilities, Krones provides the following public information:

- **Vulnerability description:** A description of the security vulnerability.
- **Rating on impact:** CVSS 3.1 Base Score or CVSS-B 4.0 score, if available.
- **Rating on exploitation:** This rating reflects known exploitation through publicly available sources, internal Krones Group knowledge, or inclusion in the CISA KEV Catalog or EUVD EV list. Alternatively, the EPSSv4 Score may be regarded as an indicator of exploitation likelihood.
- **Source:** Link to a public vulnerability source, if available.

Vulnerability CVE-2026-109618

- **Vulnerability description:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).
- **Rating on impact:** CVSS 3.1 Base Score: 9.2 (CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
- **Rating on exploitation:** actively exploited (CISA KEV), exploited (EUVD)
- **Source:** CVE Record: CVE-2026-109618

Vulnerability CVE-2026-109619

- **Vulnerability description:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).
- **Rating on impact:** CVSS-B 4.0: 9.2 (CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
- **Rating on exploitation:** actively exploited (CISA KEV), exploited (EUVD)
- **Source:** CVE Record: CVE-2026-109619

Changelog

Version	Date	Changes
1.0	2026-06-11	Originally released by the Krones Product Security Incident Response Team (PSIRT).