Security Advisory:

Mitigation Plan for CVE-2026-109618 and CVE-2026-109619 Vulnerabilities in Infosec AG/NetIAG/NetGate Products

Release Date: October 23, 2026
Beijing Infosec Technologies Co., Ltd.

Vulnerability Overview

The PHP components used in Beijing Infosec Technology Co., Ltd. AG / NetIAG / NetGate products are affected by the CVE-2026-109618 and CVE-2026-109619 vulnerabilities.

Vulnerability Descriptions

CVE-2026-109618

On October 21, 2026, the PHP official team released a security update disclosing a heap use-after-free vulnerability in its out-of-memory (OOM) error-handling mechanism. When an OOM error occurs during the request startup phase while parsing inputs such as multipart file uploads, the error-handling mechanism exits the current context via longjmp. At this point, the request memory is in a temporarily reachable, incompletely initialized state, and related states are not properly cleaned up. The request shutdown procedure subsequently reads or processes data based on this invalid state.

An unauthenticated remote attacker can send a crafted file upload request to trigger this vulnerability, leading to memory information disclosure and arbitrary code execution with web process privileges, ultimately resulting in server compromise. Successful exploitation requires the attack request to hit the same worker process, and exploit reliability depends on the PHP build, extensions, front-end behavior, and memory allocator layout.

CVE-2026-109619

On October 21, 2026, the PHP official team released a security update disclosing a heap use-after-free vulnerability in its cross-request global state management mechanism. Global states held by the PHP worker process—such as errors, sessions, objects, and extensions—point to heap memory belonging solely to a single request, which must be reset before the request memory is freed. When a request is interrupted by a fatal error (including memory exhaustion, execution timeout, etc.) without performing the corresponding reset, or when non-fatal diagnostics rewrite request-specific information into the cleaned global state during the request shutdown phase, residual references after the request heap memory is freed are still retained by the worker. Subsequent requests then execute input, configuration, session, and error-handling operations prior to normal initialization, reading or processing based on this residual state, resulting in a use-after-free condition.

An unauthenticated remote attacker can craft specialized requests processed sequentially by the same worker to trigger this vulnerability, leading to memory information disclosure and arbitrary

code execution with web process privileges, resulting in server compromise. Successful exploitation requires the relevant requests to be processed sequentially by the same worker process, and exploit reliability depends on the PHP build, extensions, front-end behavior, and heap memory layout.

CVE Threat Ratings

Metric / Vulnerability	Details
CVE-2026-109618 Threat Level	Critical
Privileges Required / Attack Vector / Attack Complexity	None / Remote / Difficult
Impact on Service Availability	Severe Impact
CVE-2026-109619 Threat Level	Critical / None / Remote / Difficult / Severe Impact

Affected Versions

Product Name	Affected Version Range
AG	9 Series: Rel AG 9.4.0.525 and earlier versions 10 Series: - Rel AG 10.3.0.32 and earlier versions - Rel_AG-HG-K 10.3.0.35 and earlier versions - Rel_AG-FTQ-K 10.3.0.34 and earlier versions
NetIAG	3 Series: - Rel NetIAG 3.4.0.32 and earlier versions - Rel NetIAG-FT-K 3.4.0.32 and earlier versions
NetGate	9 Series: Rel_NETGATE_9.4.0.87 and earlier versions 10 Series: Rel_NetGate_10_3_0_32 and earlier versions

Solutions and Mitigations

Workarounds / Mitigations

For 94XX versions of AG and NetGate products:

- (1) Global Configuration: Disable WebUI feature and Aproxy feature
  AN(config)$ webui off
  AN(config)$ vpn motionpro off
- (2) Virtual Site Configuration: Disable AAA SAML
  vs(config)$ aaa federation samlidp disable
  vs(config)$ aaa saml disable

For 103XX versions of AG and NetGate products, and 34XX versions of NetIAG products:

- (1) Virtual Site Configuration: Disable AAA SAML
  vs(config)$ aaa federation samlidp disable
- (2) Virtual Site Configuration: Ensure no 'aaa server name samlsp <Server name>' configuration exists

Resolution

Beijing Infosec Technology Co., Ltd. will release and push vulnerability patches shortly. Customers may contact Support Engineers (SE) to schedule a version upgrade accordingly.

© 2026 Beijing Infosec Technology Co., Ltd. All rights reserved.