Security Advisory:

Mitigation Plan for CVE-2026-109618 and CVE-2026-109619 Vulnerabilities in Infosec NSAE/APV/NetOpti Products

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

Vulnerability Overview

The affected versions of Infosec NSAE, APV, and NetOpti products contain vulnerabilities CVE-2026-109618 and CVE-2026-109619.

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 Required / Remote / Difficult
Impact on Service Availability	Severe Impact
CVE-2026-109619 Threat Level	Critical / None Required / Remote / Difficult / Severe Impact

Affected Versions

Product Name	Affected Version Range
NSAE / APV	• 8.6.1 Series: Version 861308 and earlier versions • 10.4.0 Series: Version 10_4_0_179_1 and earlier versions • 10.4.2 Series: Version 10_4_2_196 and earlier versions • 10.4.3 Series: Version 10_4_3_49 and earlier versions • 10.4.5 Series: Version 10_4_5_72 and earlier versions • 10.4.6 Series: Version 10_4_6_8 and earlier versions • 10.5.0 Series: Version 10_5_0_40 and earlier versions
NetOpti	• 2.6.1 Series: Version 2_6_1_65 and earlier versions • 3.4.0 Series: Version 3_4_0_179 and earlier versions • 3.4.2 Series: Version 3_4_2_177 and earlier versions • 10.4.5 Series: Version 10_4_5_72 and earlier versions • 10.5.0 Series: Version 10_5_0_40 and earlier versions

Solutions and Mitigations

Workarounds / Mitigations

For 861xx versions of NSAE/APV products and 261xx versions of NetOpti products:

- (1) Disable WebUI:
  AN(config)$ webui legacy off

For version 10 of NSAE/APV products, and versions 3 and 10 of NetOpti products:

- (1) Disable AAA SAML authentication: Delete 'aaa server name samlsp <server_name>' configuration

Resolution

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

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