

**ALE Security Advisory****No. SA-A0012****Ed. 01****CVE-2026-109618, CVE-2026-109619****Summary**

Two vulnerabilities fixed in PHP (CVE-2026-109618 and CVE-2026-109619) allow an unauthenticated remote attacker to execute arbitrary code and to obtain potentially sensitive information. At the time of writing, no public exploit and no attack in the wild have been reported.

References

<i>Reference</i>	CVE-2026-109618, CVE-2026-109619
<i>Date</i>	21/10/2026
<i>Risk</i>	High
<i>Impact</i>	execute_arbitrary_code, confidentiality
<i>Attack expertise</i>	expert
<i>Attack requirements</i>	remote_no_account_no_user_interaction
<i>CVSS score</i>	9.2 / 7.2 (informative global base & temporal scores issued by cert-ist)
<i>Affected versions</i>	PHP versions: 8.2.x prior to 8.2.35, 8.3.x prior to 8.3.36, 8.4.x prior to 8.4.27, 8.5.x prior to 8.5.12
<i>Fixed version</i>	8.2.35, 8.3.36, 8.4.27, 8.5.12

Description of the vulnerability

Several vulnerabilities have been fixed in PHP. They allow an unauthenticated remote attacker: to execute arbitrary code, to illegally take knowledge of potentially sensitive data.

Note: for vulnerability CVE-2026-109618, exploitation has been demonstrated on Apache mod_php with the default memory and input limits, before any application code is executed. According to source code analysis, PHP-FPM is also likely to be vulnerable, although no complete exploit has been demonstrated.

Note: for vulnerability CVE-2026-109619, the confirmed exploitation cases rely on the fatal_error_backtraces option (PHP 8.5) or on the session upload progress tracking feature (session.upload_progress.enabled), which is enabled by default.

Impacts

execute_arbitrary_code, confidentiality

Status on Alcatel-Lucent Enterprise Communication products

List of products and releases currently analyzed.

Products	Versions	Affected	Impact	Remediation
FlexLM	All	Under Investigation		
OmniPCX Enterprise CS	All	No		
OmniPCX Enterprise OMS	All	No		
OmniPCX Enterprise GD4	All	No		
OmniPCX Enterprise GDXL	All	No		
OmniPCX Enterprise OST-EEGW	All	No		
OmniVista 8770	All	Yes		Remediation before fix – Block use of Web directory client Fix delivery – Possibility of local quick upgrade under investigation
BootDVD (ROCKY)	All	Under Investigation		
BootDVD (SUSE)	All	Under Investigation		
OTEC / RTU2BSS	All	Yes		Fix delivery – Remediated: QA and Production environments patched.
OXESU	All	Yes	Local-access exposure only	Fix delivery – In progress: patch deployment underway.
OpenTouch				
GAS Server OS	All	Under Investigation		
VAA	All	No		
O2G	All	No		
VNA	All	No		
ALE Connect	All	Under Investigation		
ASM (Agent Selection Module)	All	Under Investigation		
Fax Server (OTFC)	All	No		
OmniPCX Record	All	No		
SelfCare	All	No		
SGA	All	No		
AVBS	All	No		
SOT	All	Under Investigation		
Dispatch Console	All	No		
Soft panel Manager	All	No		
Ticket Extractor	All	No		
CMII	All	No		
Dual Band Switching	All	No		
OXO Connect	All	Yes		Remediation before fix – see (*)
OXO Connect Evolution	All	Yes		Remediation before fix – see (*)
OCE Front-End	All	Yes		Remediation before fix – see (*)
OMC / OHL / OLD / PIMPhony / AST / LabelSet	All	Under Investigation		

8088	All	Under Investigation		
8008/G	All	No		
ALE Enterprise DeskPhones (ALE-500 / 400 / 300) - NOE	All	Under Investigation		
ALE Enterprise DeskPhones (ALE-500 / 400 / 300) - SIP	All	Under Investigation		
ALE Essential DeskPhones (ALE-30H / 20H / 20) - NOE	All	Under Investigation		
ALE-2 / ALE-3	All	No		
ALE-160 (Bluetooth handset)	All	Under Investigation		
8135s / 800 / 8105s EGO	All	Under Investigation		
WLAN handset 8158s / 8168s	All	Under Investigation		
WLAN Tools Winpdm	All	Under Investigation		
WLAN Tools IMS3	All	Under Investigation		
8212 (DECT handsets)	All	No		
8262/62ex (DECT handsets)	All	No		
8214 (DECT handsets)	All	No		
8244 (DECT handsets)	All	No		
8234/8254 (DECT handsets)	All	No		
82x2/82x4 DECT Handset Unified Support Tool (UST)	All	No		
8378 (IP-xBS)	All	No		
8379 (IBS renewal + IBS ATEX)	All	Under Investigation		
8318 (SIP-DECT Firmware)	All	No		
EDS / EPS / EDM	All	Under Investigation		
8008-CE / 8008G-CE / 8018 CE / 80x8s CE	All	Under Investigation		
M3 / M5 / M7	All	Under Investigation		
H2	All	Under Investigation		
H3 / H6 / M8	All	Under Investigation		
EM20 / EM200	All	Under Investigation		

Status on Alcatel Lucent Enterprise Rainbow solutions

List of products and releases

Products	Versions	Affected	Impact	Remediation
Rainbow UCaaS/CPaaS/Edge/HDS/Hub	All	No		
WebRTC gateway	All	No		
Rainbow for Developers Portal	All	No		
SDK NodeJS & C#	All	No		
Rainbow Exporter	All	No		
Rainbow Hospitality	All	No		
Rainbow Classroom	All	No		
Rainbow Pilot	All	No		
Rainbow CRM Bridge	All	No		

Rainbow Compliance Recorder	All	No		
RcaaS	All	No		
Kiosk	All	No		
SafetyZone	All	No		
C2C RVA	All	No		
Caixa Mobile	All	No		
Pexip / HZD	All	No		

Status on Alcatel-Lucent Enterprise Network products

<i>Products</i>	<i>Versions</i>	<i>Affected</i>	<i>Remediation</i>
Subscription Manager	All	No	NA
Asset Tracking	All	No	NA
OV Cirrus (4.x)	All	No	NA
OV Cirrus (1x.x)	All	No	NA
OV 2500	All	No	NA
RAP Appliance	All	No	NA
OmniSwitch AOS 5 (2x60)	All	Under Investigation	
OmniSwitch AOS 6 (6250, 6350, 6450)	All	No	NA
OmniSwitch AOS 8 (6360, 6465, 6560, 6570, 6860, 6865, 6870, 6900, 6920, 9900)	All	Under Investigation	
OmniAccess Stellar AP	All	No	NA
OmniVista Network Advisor	All	No	NA
AOS 10	All	No	NA
OmniSmart tool	All	No	NA
OmniVista Terra	All	No	NA
License Activation Server	All	No	NA
Fleet Supervision	All	No	NA

(*) Since OXO Webdiag is accessible from the Internet, as a precautionary measure, we advise customers to disable WAN access until the PHP upgrade is completed. This can be configured via OMC:

OMC → Security → Network IP Services → under User Services → Disable "Allow User Application Services from WAN"

History

Version	Date	History
01	22/10/2026	creation