PHP2Shell sårbarheter

Säkerhetsinformation från COBS

COBS AB | 27 oktober 2026
Berörda system, produktstatus och åtgärder för kund

1 Om denna information

Denna information vänder sig till kunder med system levererade av COBS och avser de PHP-sårbarheter som i underlaget benämns PHP2Shell: **CVE-2026-109618 och CVE-2026-109619**. Syftet är att beskriva vilka system som kan vara berörda och vilka åtgärder som kan behövas i kundens installation.

Informationen bygger på COBS produktunderlag och återgivna leverantörsbesked. Bedömningen gäller enbart de angivna sårbarheterna och är inte ett generellt besked om systemens säkerhet. Installerad produkt, programvaruversion och eventuella tillägg behöver kontrolleras för respektive installation. Huvuddokumentet omfattar berörda produkter. Övriga produktbesked och avgränsningar finns i Appendix A.

- **COBS CMS:** Berört enligt COBS underlag. Uppdatering behöver planeras.
- **Zenitel ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE och Exigo:** Angivna versioner är berörda. Begränsa administrationsåtkomsten och vidta produktspecifika åtgärder enligt nedan.

Bakgrund: Enligt säkerhetsmeddelande offentliggjorde PHP-projektet sårbarheterna den 21 oktober 2026. Båda klassas som kritiska med CVSS v4.0 9,2 av 10 och avser fel i PHP:s minneshantering. De kan möjliggöra fjärrkörning av kod utan autentisering via ett åtkomligt PHP-baserat webbgränssnitt, med webbserverprocessens behörigheter. Utnyttjande är enligt meddelandet komplext och beroende av webbserverns konfiguration. COBS känner vid denna publicering inte till att något utnyttjande skett i dessa produkter.

1.1 Produktstatus och kundåtgärder

1.1.1 COBS CMS

Status: Berört. COBS CMS behöver uppdateras för att åtgärda de angivna sårbarheterna. **Åtgärd för kund:** Säkerhetsuppdatering till programvaruversion **v4.05** för CMS III och CMS IV finns nu tillgänglig på COBS Supportportal för nedladdning per den 2026-10-27. Äldre och utfasade CMS system (I & II) behöver bytas till ny CMS IV MkII.

1.1.2 Zenitel

Status: Angivna produkter och versioner är berörda. Zenitels säkerhetsmeddelande A100K12410, revision 1.0, daterat den 23 oktober 2026, omfattar ICX-AlphaCom, ICX-AlphaCom Core, AlphaCom XE och Exigo (systemstyrenheter ICX-500, ICX-510 och ESC1 inklusive AMC-IP). Versionsgränser och åtgärder framgår nedan. Uppdateringsdatumen i

meddelandet var planerade datum, inte bekräftelser på publicerade uppdateringar. Faktisk tillgänglighet behöver bekräftas med COBS eller Zenitel.

Produktfamilj	Berörda versioner	Åtgärdsstatus enligt meddelandet
ICX-AlphaCom	Alla versioner till och med 1.5.3.7	Säkerhetsuppdatering under utveckling; planerad till 2026-10-23. Bekräfta tillgänglighet. Begränsa administrationsåtkomsten omgående.
ICX-AlphaCom Core	Alla versioner till och med 1.5.3.7 på Ubuntu 22.04 LTS	Rättade PHP-paket finns enligt meddelandet via Ubuntu: php8.1 8.1.2-1ubuntu2.28 eller senare (USN-8948-1). Installera Ubuntus säkerhetsuppdatering snarast.
AlphaCom XE	Alla versioner till och med 13.2.3.16	Tillämpa permanenta nätverksbegränsningar. Ingen rättad PHP-version anges som tillgänglig för denna plattform.
Exigo	Alla versioner till och med 1.7.3.7 Alla versioner till och med 2.0.3.1	Säkerhetsuppdatering för Exigo-systemstyrenheter under utveckling; planerad senast 2026-10-26. För ESC1 inklusive AMC-IP anges endast nätverksbegränsningar som tillgänglig åtgärd. Se nedan.

Gemensamma åtgärder för berörda Zenitel-produkter: Begränsa HTTP/HTTPS-åtkomst till det webbaserade administrationsgränssnittet till betrodda administrationsnät och administratörers arbetsstationer, med brandväggsregler och separat administrations-VLAN. Exponera inte gränssnittet mot internet eller obetrodda nät. Använd VPN eller motsvarande autentiserad och krypterad anslutning vid fjärradministration. Kontrollera oväntade omstarter av webbgränssnittet, konfigurationsändringar och användarkonton. Rapportera misstänkt aktivitet till Zenitels produktsäkerhetsfunktion, security@zenitel.com.

1.1.2.1 ICX-AlphaCom

Berörda versioner: Alla versioner till och med 1.5.3.7.
Åtgärd för kund: Tillämpa de gemensamma nätverksbegränsningarna omgående och installera Zenitels säkerhetsuppdatering när den finns tillgänglig. Meddelandet anger en planerad uppdatering den 23 oktober 2026, men bekräftar varken publicering eller rättat produktversionsnummer. Kontakta COBS för att bekräfta tillgänglig version och uppdateringsväg. Ubuntu-åtgärden i nästa avsnitt gäller ICX-AlphaCom Core.

1.1.2.2 ICX-AlphaCom Core

Berörda versioner: Alla versioner till och med 1.5.3.7 som körs på Ubuntu 22.04 LTS.
Åtgärd för kund: Installera snarast Ubuntus säkerhetsuppdatering USN-8948-1 i den virtuella maskinen. Zenitel anger version 8.1.2-1ubuntu2.28 eller senare för berörda PHP 8.1-paket: libapache2-mod-php8.1, php8.1-cgi, php8.1-cli och php8.1-fpm. PHP tillhandahålls av Ubuntu och uppdateras inte genom ICX-AlphaCom Core-versioner. Kunden ansvarar för att hålla den virtuella maskinens Ubuntu-operativsystem uppdaterat. Samordna med ansvarig driftorganisation och tillämpa även de gemensamma nätverksbegränsningarna.

1.1.2.3 AlphaCom XE

Berörda versioner: Alla versioner till och med 13.2.3.16.
Åtgärd för kund: Tillämpa de gemensamma nätverksbegränsningarna permanent. Enligt

Zenitels meddelande används PHP 5.6.38, för vilken ingen rättad version fanns vid publiceringen. Nätverksbegränsningar anges som den enda tillgängliga riskbegränsande åtgärden.
Fortsatt hantering: Zenitel rekommenderar att planera migrering från AlphaCom XE till ICX-AlphaCom. Kontakta COBS för installationsspecifik planering.

1.1.2.4 Exigo

Berörda versioner: Alla versioner till och med 1.7.3.7 respektive 2.0.3.1 enligt Zenitels produkttabell.
Åtgärd för kund: Tillämpa de gemensamma nätverksbegränsningarna omgående. För Exigo-systemstyrenheter anger meddelandet en säkerhetsuppdatering under utveckling, med planerad tillgänglighet senast den 26 oktober 2026. Datumet är inte en bekräftelse på publicering; kontrollera aktuell tillgänglighet och rätt uppdateringsväg med COBS eller Zenitel.
ESC1 inklusive AMC-IP: Dessa anges separat använda PHP 5.6.38 utan tillgänglig rättad version vid publiceringen. För dessa anges nätverksbegränsningar som den enda tillgängliga åtgärden och de ska tillämpas permanent. Utgå inte från att den planerade Exigo-uppdateringen omfattar dessa enheter utan produktspecifik bekräftelse.

1.1.2.5 Övriga Zenitel-produkter

Enligt Zenitels säkerhetsmeddelande A100K12410, revision 1.0, daterat den 23 oktober 2026, påverkas inga andra Zenitel-produkter än de produktfamiljer och systemstyrenheter som anges i huvuddokumentets Zenitel-avsnitt. Beskedet gäller endast de två angivna PHP-sårbarheterna.

Kontakt och fortsatt hantering

Om ni är osäkra på vilka produkter eller versioner som ingår i er installation, kontakta COBS. Ange gärna anläggning, produktbeteckning och installerad programvaruversion så att rätt åtgärd kan fastställas. Uppdateringar och nätverksändringar bör samordnas med ansvarig driftorganisation och COBS för att ta hänsyn till installationens funktion och tillgänglighet.

COBS AB
Telefon: +46 (0)31-33 33 840
E-post: support@cobs.se

2 Appendix A – Övriga IP-baserade produkter och avgränsningar

Här samlas produkter som enligt befintligt underlag inte är berörda samt besked med undantag eller behov av separat bedömning. Beskeden gäller endast CVE-2026-109618 och CVE-2026-109619. Att en komponent inte är berörd innebär inte att hela det sammankopplade systemet är opåverkat.

2.1 COBS Alert4U2 – A-TRAX IP

Status: Inte berört. A-TRAX IP-sändare och -mottagare använder inte PHP.
Åtgärd för kund: Ingen åtgärd krävs på dessa komponenter med anledning av de angivna sårbarheterna. Om installationen även innehåller COBS CMS gäller åtgärderna i CMS-avsnittet för den delen av systemet.

2.2 Moxa NPort

Status: Inte berört. Moxa uppger att inga av företagets produkter påverkas av dessa sårbarheter.
Åtgärd för kund: Ingen åtgärd krävs på Moxa NPort med anledning av de angivna sårbarheterna.

2.3 Modbus-relaterade produkter

Status: Inte berört. uppger att inga av företagets produkter påverkas av dessa sårbarheter.
Åtgärd för kund: Ingen åtgärd krävs på Modbus-relaterade enheter med anledning av de angivna sårbarheterna.

2.4 Funktel Nucleus

Status: Inte berört. PHP installeras inte som standard på Nucleus-plattformen och används inte av Nucleus.
Åtgärd för kund: Ingen åtgärd krävs för Nucleus i standardutförande med anledning av dessa sårbarheter. Beskedet omfattar inte eventuell separat installerad PHP-programvara.

2.5 COBS MOBILE

Status: Inte berört. Dessa plattformar använder inte PHP.
Åtgärd för kund: Ingen åtgärd krävs för dessa plattformar med anledning av de angivna sårbarheterna.

2.6 COBS CWS DECT

Status: Inte berört. Varken DECT-system, inklusive administrationsgränssnittet AMIE för DECT använder PHP.
Åtgärd för kund: Ingen åtgärd krävs för dessa produkter med anledning av de angivna sårbarheterna. Eventuellt anslutet COBS CMS behöver bedömas separat.

2.7 2N

Status: Inte berört. Leverantören uppger att en intern analys har bekräftat att inga 2N-produkter påverkas av de angivna sårbarheterna.

Åtgärd för kund: Ingen åtgärd krävs för 2N:s produkter och lösningar med anledning av dessa sårbarheter.

2.8 Innovaphone

Status: Inte berört, med undantag för äldre v10 App Platform. Innovaphone uppger att produkterna inte använder PHP, förutom den äldre v10 App Platform som inte längre stöds. Beskedet om att produkterna inte påverkas ska därför inte tillämpas på denna äldre plattform.
Åtgärd för kund: Ingen åtgärd krävs för de produkter som omfattas av beskedet om att PHP inte används. Kunder med v10 App Platform bör kontakta COBS för separat bedömning och fortsatt hantering.
Leverantörens tjänster: Innovaphone uppger att vissa egna tjänster påverkades och att webbplatser togs ned i väntan på uppdatering. Driftinformation hänvisas till status.innovaphone.com.