Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Internet: phoenixcontact.com
Telefon: +49 5235 300
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

Phoenix Contact GmbH & Co. KG · 32825 Blomberg

Vulnerabilities in PHP - PHP2Shell

The designation PHP2Shell refers to the PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619. Under certain conditions, these vulnerabilities can be exploited by unauthenticated attackers to execute commands on an affected system.
Phoenix Contact has investigated the potential impact on its products. This investigation identified products affected by these vulnerabilities.

Recommended measures

Until corrected firmware becomes available, Phoenix Contact recommends restricting network access to affected devices to the connections necessary for operation. In particular, affected devices should not be directly accessible from public or untrusted networks.
In addition, we recommend consistently implementing the protective measures described in our “INDUSTRIAL SECURITY” user note. These include, in particular, network segmentation, the use of suitable firewalls, the restriction of access rights, and the use of up-to-date firmware versions.

Firmware updates

Phoenix Contact will provide firmware updates for affected devices in its current product portfolio. Once available, these updates will be available for download on the respective Phoenix Contact product pages. In parallel, Phoenix Contact will publish a security advisory on the PSIRT website.
For products that are no longer part of the current product portfolio, Phoenix Contact will assess for each product whether a firmware update can be provided. If no firmware update is available, Phoenix Contact particularly recommends consistently implementing the protective measures outlined above.

Affected products

Based on current knowledge, the products or product families listed on the last page of this document are affected.

Sicherheitslücken in PHP - PHP2Shell

Unter der Bezeichnung PHP2Shell werden die Schwachstellen CVE-2026-109618 und CVE-2026-109619 in PHP zusammengefasst. Unter bestimmten Voraussetzungen können nicht authentifizierte Angreifer diese Schwachstellen ausnutzen, um Befehle auf einem betroffenen System auszuführen. Phoenix Contact hat untersucht, welche Auswirkungen die Schwachstellen auf seine Produkte haben könnten. Dabei wurden Produkte identifiziert, die von den Schwachstellen betroffen sind.

Empfohlene Maßnahmen
Bis eine korrigierte Firmware verfügbar ist, empfiehlt Phoenix Contact, den Netzwerkzugriff auf betroffene Geräte auf die für den Betrieb notwendigen Verbindungen zu beschränken. Insbesondere sollten betroffene Geräte nicht direkt über öffentliche oder nicht vertrauenswürdige Netzwerke erreichbar sein.
Darüber hinaus empfehlen wir, die in unserem Anwenderhinweis „INDUSTRIAL SECURITY“ beschriebenen Schutzmaßnahmen konsequent umzusetzen. Dazu gehören insbesondere die Netzwerksegmentierung, der Einsatz geeigneter Firewalls, die Beschränkung von Zugriffsrechten sowie die Verwendung aktueller Firmware-Versionen.

Firmware-Updates
Für betroffene Geräte aus dem aktuellen Produktportfolio wird Phoenix Contact Firmware-Updates bereitstellen. Sobald diese verfügbar sind, werden sie auf den jeweiligen Produktseiten von Phoenix Contact zum Download bereitgestellt. Parallel dazu veröffentlicht Phoenix Contact ein Security-Advisory auf der PSIRT-Webseite.

Für Produkte, die nicht mehr zum aktuellen Produktportfolio gehören, wird für jedes Produkt geprüft, ob ein Firmware-Update bereitgestellt werden kann. Ist kein Firmware-Update verfügbar, empfiehlt Phoenix Contact insbesondere die oben genannten Schutzmaßnahmen konsequent umzusetzen.

Betroffene Produkte
Nach aktuellem Kenntnisstand sind die auf der letzten Seite dieses Dokuments genannten Produkte beziehungsweise Produktfamilien betroffen.

Affected products or product families / Betroffene Produkte bzw. Produktfamilien:

Product family	Fixed version	Release date
FL WLAN 1x2x/23xx	26.10	2026-11-18
FL SWITCH 2xxx	3.60	2026-11-18
FL NAT 2xxx	3.60	2026-11-18
FL SWITCH TSN 23xx	3.60	2026-11-18
FL SWITCH 59xx	3.60	2026-11-18
TC ROUTER 4xxx	5.0.72.105	2026-12-02
FL TIMESERVER NTP	5.0.71.105	2026-12-02
FL WLAN 11xx/21xx	No fix planned	-
TC EXTENDER x00x	No fix planned	-
SCX xPOE	No fix planned	-