

SECURITY ADVISORY



Information about critical php2shell vulnerabilities CVE-2026-109618 and CVE-2026-109619

Advisory ID	CSA-2026-72
Title	Information about critical php2shell vulnerabilities CVE-2026-109618 and CVE-2026-109619
Devices	• Symphony Cloud (Ivy Dashboard) and • Commend Customized Solutions products ("Y" articles) with built-in ENEO cameras: ◦ ISM-52F0021WM* (current model) ◦ ISM-52F0021W0A (discontinued 11.2022) ◦ NXP-880F* (discontinued 04.2020)
Severity	Critical
CVSS score	9.2
CVSS base	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
First published	22.10.2026
Last updated	22.10.2026
Version	1.0

Summary of vulnerability notification

Various news outlets reported critical vulnerabilities in PHP (php2shell).

The Ivy Dashboard of Symphony Cloud WAS affected. The security-related fixes and updates for these vulnerabilities have been applied on 22nd of October 2026 at 09:45 (GMT+2).

The following Commend Customized Solutions products ("Y" articles) with built-in ENEO cameras ARE affected:

- ISM-52F0021WM* (current model)
- ISM-52F0021W0A (discontinued 11.2022)
- NXP-880F* (discontinued 04.2020)

Download the patches as they become available from <https://www.videor.com/en/>

Note: The following Commend products are NOT AFFECTED, as they do NOT use PHP:

- CCT 800
- ComLOG
- ComOPC Server
- Customized Solutions software (ComPLC, WebVisu, APM)
- EE 980
- IP Station Config
- Set-UP
- Studio
- Symphony BF
- Symphony Configuration and Symphony Uplink
- Symphony MX
- WS stations with built-in AXIS camera:
 - WS 20xPI CA
 - WS 20xVI CA
 - WS 21xVI CA
- EM 6CA
- VirtuoBRO
- VirtuoSIS, S6, S3
- VirtuoSIS Link

Affected products

- Symphony Cloud (Ivy Dashboard)
- Commend Customized Solutions products ("Y" articles) with ENEO cameras:
 - ISM-52F0021WM* (current model)
 - ISM-52F0021W0A (discontinued 11.2022)
 - NXP-880F* (discontinued 04.2020)

Software updates

- Symphony Cloud (Ivy Dashboard) on 22nd of October 2026 at 09:45 (GMT+2), automatically delivered
- For the Commend Customized Solutions products ("Y" articles) with built-in ENEO cameras, download the patches as they become available from <https://www.videor.com/en/>.

Workaround

Disconnect the ENEO camera from the public IP network.

Exploitation and public announcements

The Commend Security Board is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Acknowledgement

-

Sources

Information about the vulnerability notification can be found at the following sources:

<https://nvd.nist.gov/vuln/detail/cve-2026-109618>

<https://nvd.nist.gov/vuln/detail/cve-2026-109619>

Contact and coordinated disclosure

support@commend.com

COMMEND INTERNATIONAL GMBH
Saalachstraße 51
5020 Salzburg, Austria

Change log

- 21.10.2026 – External finding
- 22.10.2026 – Vulnerability confirmed
- 22.10.2026 – Vulnerability for Symphony Cloud (Ivy Dashboard) fixed and fix verified
- 22.10.2026 – First published