



SECURITY ADVISORY

SPR-261027-7, Ausgabe 2

27. Oktober 2026

Sprecher Automation GmbH
Franckstraße 51, 4020 Linz / Österreich
Tel. +43 732 6908-0
Fax +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

Inhaltsverzeichnis

1.	Zusammenfassung	2
2.	Betroffene Produkte und Versionen.....	2
3.	Workarounds und Mitigationen	2
4.	Schwachstellen-Klassifizierung	3
5.	Allgemeine Sicherheitsempfehlungen	3
6.	Sprecher Automation PSIRT	3
7.	Dokumentenverlauf	4

Copyright: Sämtliche Inhalte wie z.B. Texte, Namen, Konfigurationen, Bildnisse sowie Layouts, Designs, Logos und Grafiken sind urheberrechtlich oder durch andere anwendbare Rechte geschützt. Änderungen, Druckfehler, Irrtümer sowie alle Rechte bleiben jederzeit vorbehalten.

Haftungsausschluss: Dieses Dokument enthält allgemeine Analysen und Klassifizierungen und ist nicht auf die konkreten Anlagen und Konfigurationen des Kunden zugeschnitten. Die Informationen und Angaben sind ausschließlich Empfehlungen und vom Kunden sinngemäß auf die eigenen Anlagen und Konfigurationen anzuwenden und nach eigenem Ermessen in eigener Verantwortung umzusetzen. Eine Haftung oder Gewähr für deren Richtigkeit oder Vollständigkeit kann nicht übernommen werden.

SPRECON-NDM: Critical Vulnerabilities in PHP

1. Zusammenfassung

Das Kernsystem des SPRECON-NDM **ist nicht betroffen**: Die Kernarchitektur und die Web-GUI von Checkmk basieren auf Python/C++ und nutzen kein PHP. **Betroffen ist die Komponente NagVis**, die Checkmk für Netzwerk-Maps einbindet: Sie basiert auf PHP und greift auf die PHP-Pakete des Host-Betriebssystems zu. NagVis lauscht auf keinem separaten Port, ist jedoch über den Webserver unter dem Pfad /nagvis/ erreichbar (standardmäßig durch das Checkmk-Login geschützt). Sind die PHP-Pakete des Host-Betriebssystems nicht gepatcht, besteht hierüber ein potenzielles Angriffsrisiko.

2. Betroffene Produkte und Versionen

SPRECON-NDM

3. Workarounds und Mitigationen

Host-Betriebssystem patchen (empfohlen): Aktualisieren Sie die PHP-Pakete auf dem Linux-Host (apt upgrade php* bzw. dnf upgrade php*). Dadurch wird die Schwachstelle direkt an der Wurzel behoben.

NagVis temporär deaktivieren (Sofortmaßnahme ohne Reboot/OS-Patch): Falls ein OS-Patching kurzfristig nicht möglich ist oder NagVis nicht aktiv genutzt wird, lässt sich die PHP-Komponente pro Checkmk-Site vollständig abschalten:

- Schritt 1

```
omd stop omd config set NAGVIS OFF omd start
```
- Schritt 2
 - Site-internen PHP-FPM prüfen

```
omd shell -- <site>
ps aux | grep -i '[p]hp-fpm'
exit
```
 - System-eigenen PHP-FPM am Host stoppen und deaktivieren

```
systemctl stop php*-fpm
systemctl disable php*-fpm
```
 - Verifikation

```
ps aux | grep -i '[p]hp'
→ Keine Ausgabe erwartet
curl -sk -o /dev/null -w "%{http_code}\n" https://<host>/nagvis/
→ Ausgabe: 404/403
curl -sk -o /dev/null -w "%{http_code}\n" https://<host>/test.php
→ Ausgabe: 404/403
```

Damit werden keine PHP-Inhalte mehr über Checkmk ausgeliefert und der Angriffsvektor ist geschlossen.

4. Schwachstellen-Klassifizierung

CVE ID: CVE-2026-109618 / CVE-2026-109619

CVSS 4.0 Score: 9.2 (CRITICAL)

CVSS Vektor: 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

Das CVE®-Programm identifiziert, definiert und katalogisiert öffentlich bekannt gemachte Sicherheitslücken im Bereich der Cybersicherheit. Die Schwachstellen werden von Organisationen aus der ganzen Welt, die eine Partnerschaft mit dem CVE®-Programm eingegangen sind, entdeckt, zugewiesen und veröffentlicht. (Copyright © The MITRE Corporation <https://www.cve.org/Legal/TermsOfUse>)

CVSS ist ein offener Bewertungsrahmen, mit dem die Merkmale und der Schweregrad von Software-Schwachstellen angegeben werden können, wobei dies kein Maß für das Risiko ist. Dieser Standard ist auf der Website <https://www.first.org/cvss/> dokumentiert.

5. Allgemeine Sicherheitsempfehlungen

Sprecher Automation empfiehlt die Einhaltung üblicher Sicherheitsempfehlungen allgemeiner und branchenspezifischer Standards und Normen wie z. B.:

- den lokalen physischen Zugang nur auf autorisierte Personen zu beschränken
- das Betriebssystem und die Software auf dem neuesten Stand zu halten
- Verwendung von Anwendungs-Whitelisting, um die Ausführung von Anwendungen auf die für den Betrieb des Systems erforderlichen Anwendungen zu beschränken
- das Testen von aktualisierten Versionen in einer Testumgebung, um den normalen Betrieb des Systems gemäß der projektspezifischen Konfiguration und Hardwareumgebung zu überprüfen, bevor das Update in einer Produktionsumgebung installiert wird
- dass ein Notfallplan vorhanden ist, um die Installation der Aktualisierung rückgängig zu machen, falls nach der Installation des Updates unerwartete Probleme in der Produktionsumgebung auftreten

6. Sprecher Automation PSIRT

Sprecher Automation hat ein **Product Security and Incident Response Team (PSIRT)**, um Risiken zu reduzieren, Cybersicherheit in den Produkten zu erhöhen und um IT Security-Zwischenfälle aufzulösen. Haben Sie oder Ihr Unternehmen eine Cybersicherheits-Schwachstelle in Produkten von Sprecher Automation gefunden, kontaktieren Sie uns bitte an der Funktionsadresse security@sprecher-automation.com. (Sollten Sie ein S/MIME-Zertifikat für verschlüsselte Kommunikation benötigen, können Sie ein E-Mail mit dem Betreff „Zertifikatsrequest“ an diese Adresse schicken.)

7. Dokumentenverlauf

2026-10-22 Ausgangsdokument

2026-10-27 Mitigation, Rating