CNEXT SECURITY SERVICES · ERSTMELDUNG · IM VORFALL

Erstmeldung Sicherheitsvorfall

KUNDE
Muster AG, Bern (erfunden)

VORFALL
INC-2026-041, Schwachstelle in SharePoint Server, aktiv ausgenutzt

GEMELDET AM
Dienstag, 14. April 2026, 21:40

STUFE
Kritisch, bestätigt durch CNEXT

1	3	08:00	2
betroffenes System	Sofortmassnahmen	nächste Information	Personen erreicht

Wann Sie dieses Dokument erhalten: Innerhalb der im Alarmplan vereinbarten Zeit, per Mail und Telefon.

Zusammenfassung

Microsoft hat heute ein Sicherheitsupdate für SharePoint Server 2016, 2019 und Subscription Edition veröffentlicht. Die Lücke wird bereits im Internet ausgenutzt; sie braucht weder Anmeldung noch Benutzeraktion. Ihr Inventar führt SRV-SP01 mit SharePoint Server 2019 und Zugriff aus dem Internet über das Partnerportal. Wir stufen den Fall als kritisch ein.

Sofortmassnahmen

NR.	MASSNAHME	WER	BIS
1	Partnerportal auf SRV-SP01 am Reverse Proxy sperren, bis das Update installiert ist	IT Muster AG	heute 22:30
2	Sicherheitsupdate KB für SharePoint Server 2019 im Wartungsfenster installieren, Konfigurations-Assistent ausführen	IT Muster AG mit CNEXT	Mi 15. April, 07:00
3	IIS- und ULS-Protokolle seit 1. April auf die bekannten Anfragemuster prüfen	CNEXT	Mi 15. April, 10:00

Kontakt und nächste Information

- Ihre Ansprechperson bei CNEXT ist heute Abend und morgen ab 07:00 unter der Nummer aus dem Alarmplan erreichbar.
- Nächster Lagebericht: Mittwoch, 15. April 2026, 08:00, per Mail an die Kontaktkette.
- Quelle: Microsoft Security Update Guide, Eintrag vom 14. April 2026; CISA hat die Lücke in den Katalog ausgenutzter Schwachstellen aufgenommen.

So geht es weiter

Bitte bestätigen Sie den Erhalt per Antwort auf diese Mail oder telefonisch. Massnahme 1 setzen Sie heute Abend um; Massnahme 2 und 3 begleiten wir morgen früh.

Alle Namen, Systeme und Zahlen in diesem Dokument sind erfunden. Ihr Bericht enthält Ihre Umgebung am Tag der Prüfung.