CNEXT SECURITY SERVICES · INITIAL ALERT · DURING AN INCIDENT

Initial security incident alert

CUSTOMER
Muster AG, Bern (fictional)

INCIDENT
INC-2026-041, vulnerability in SharePoint Server, actively exploited

REPORTED ON
Tuesday, 14 April 2026, 21:40

LEVEL
Critical, confirmed by CNEXT

1	3	08:00	2
system affected	immediate measures	next update	people reached

When you receive this document: Within the time agreed in the alert plan, by email and phone.

Summary

Microsoft has published a security update for SharePoint Server 2016, 2019 and Subscription Edition today. The vulnerability is already being exploited on the internet; it needs neither sign-in nor user interaction. Your inventory lists SRV-SP01 with SharePoint Server 2019 and access from the internet through the partner portal. We rate the case as critical.

Immediate measures

NO.	MEASURE	WHO	BY
1	Block the partner portal on SRV-SP01 at the reverse proxy until the update is installed	Muster AG IT	today 22:30
2	Install the security update KB for SharePoint Server 2019 in the maintenance window, run the configuration wizard	Muster AG IT with CNEXT	Wed 15 April, 07:00
3	Check IIS and ULS logs since 1 April for the known request patterns	CNEXT	Wed 15 April, 10:00

Contact and next update

- Your contact at CNEXT is reachable this evening and tomorrow from 07:00 at the number in the alert plan.
- Next status report: Wednesday, 15 April 2026, 08:00, by email to the contact chain.
- Source: Microsoft Security Update Guide, entry of 14 April 2026; CISA has added the vulnerability to its catalog of known exploited vulnerabilities.

Next steps

Please confirm receipt by replying to this email or by phone. You implement measure 1 this evening; we accompany measures 2 and 3 tomorrow morning.

Every name, system and number in this document is invented. Your report contains your environment on the day of the check.