CNEXT SECURITY SERVICES · CLOSING REPORT · DURING AN INCIDENT

Closing report

CUSTOMER
Muster AG, Bern (fictional)

INCIDENT
INC-2026-041, vulnerability in SharePoint Server

DURATION
14 April 2026, 21:40 to 15 April 2026, 16:10

OUTCOME
Closed, no exploitation found

18 h	4	0	3
from alert to closure	measures	reports to authorities needed	lessons

When you receive this document: Within a week of closing the incident.

Summary

The vulnerability was reported 2 hours 10 minutes after publication, the affected portal blocked 40 minutes after the initial alert and the server updated the next morning. The check of the logs since 1 April showed no traces of exploitation. According to our check no personal data left the system; a report to the FDPIC or BACS was not indicated. The portal has been reachable again since 16:10.

Timeline

TIME	EVENT	WHO
14 Apr 19:30	Microsoft publishes the security update; the agent reads the entry in the Security Update Guide	Agent
14 Apr 19:34	Match against the inventory: SRV-SP01 affected, reachable from the internet; proposal critical	Agent
14 Apr 21:25	Rating reviewed and confirmed, initial alert written	CNEXT
14 Apr 21:40	Initial alert by email and call to IT lead and deputy	CNEXT
14 Apr 22:20	Partner portal blocked	Muster AG IT
15 Apr 07:50	Update installed, configuration wizard completed	Muster AG IT with CNEXT
15 Apr 15:40	Log check completed, no traces	CNEXT
15 Apr 16:10	Portal released, incident closed	Muster AG IT

Lessons and changes

- The reverse proxy had no prepared rule for blocking individual sites; the rule now exists and is linked in the alert plan.
- SharePoint Server 2019 reaches end of support on 14 July 2026; the move to SharePoint Online is listed in the inventory as a project with a date.
- The deputy of the IT lead was reachable only by email in the evening; the alert plan now lists a second phone number.

Next steps

This report goes to management and the IT lead and is listed among the cases in the April monthly report.

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