

Security Advisor: CVE-2026-42897

Exchange Server OWA Spoofing — Active Exploitation, No Patch

Field	Value
Prepared by	Centrio AS on behalf of nLogic AS
Author	Kim Hansen — Security Advisor
Date issued	17 May 2026
Classification	Customer deliverable / internal reference
Status	Actively exploited. Temporary mitigation via Exchange EMS. No security update yet.
CVSS	8.1 (High)
CISA KEV	Added 15 May 2026 — FCEB deadline 29 May 2026

1. Executive Summary

CVE-2026-42897 is a spoofing vulnerability in Microsoft Exchange Server Outlook Web Access (OWA), caused by a cross-site scripting flaw in how OWA renders incoming messages. An attacker who sends a specially crafted email can cause arbitrary JavaScript to execute in the OWA browser context when the recipient opens the message, leading to session hijacking, credential theft, or manipulation of mailbox content.

Microsoft confirmed active exploitation on **14 May 2026**, two days after the May Patch Tuesday — which was widely reported as the first zero-day-free Microsoft security update since June 2024. CISA added CVE-2026-42897 to the Known Exploited Vulnerabilities catalog on 15 May 2026 with a federal remediation deadline of **29 May 2026**.

Affected products

- Microsoft Exchange Server 2016 (all Cumulative Updates)
- Microsoft Exchange Server 2019 (all Cumulative Updates)
- Microsoft Exchange Server Subscription Edition

Not affected

- Microsoft 365 / Exchange Online (does not share the affected OWA codebase)
- Outlook for Windows, Outlook for Mac, Outlook Mobile (when not used via OWA)

Conditions for exploitation

- Recipient mailbox hosted on a vulnerable on-premises Exchange Server
- Recipient opens the crafted email in Outlook Web Access (browser)
- No prior authentication on the attacker's part — only the ability to send mail to the target

Effective mitigations available now

1. Exchange Emergency Mitigation Service (EMS) — Microsoft published the automatic mitigation CVE-2026-42897-M2 (internal ID M2.1.x). EMS is enabled by default since September 2021 and pulls the mitigation automatically when the server has outbound HTTP to officecdn.microsoft.com.
2. Exchange On-premises Mitigation Tool (EOMT) — manual fallback for air-gapped environments or organizations with EMS disabled.
3. Compensating controls — Conditional Access on OWA, MFA enforcement, WAF rules to inspect OWA traffic, and disabling external OWA access for high-risk users until a security update ships. A formal Microsoft security update is expected in a subsequent monthly or out-of-band release. This advisory will be revised when the patch is released.

2. Technical Detail

2.1 Vulnerability Class

CVE-2026-42897 is classified by Microsoft as a spoofing vulnerability but the underlying flaw is a stored / reflected XSS in OWA's message rendering pipeline. The vulnerable code path fails to sanitize specific encoded payloads in message bodies, allowing JavaScript to execute in the browser's OWA origin when the recipient opens the message.

The "spoofing" framing reflects the practical attacker outcome: because the script runs in the OWA context, the attacker can render arbitrary content as if it originated from Exchange itself — including faked banking confirmations, internal HR notices, or manipulated display of trusted senders.

2.2 Attack Chain

4. Delivery. Attacker sends a crafted email to a target whose mailbox is on a vulnerable on-premises Exchange Server. No authentication required.
5. Rendering. The email passes through Exchange transport without rejection (the malicious payload is structurally valid email).
6. Execution. The recipient opens the message in OWA. The unsanitized payload triggers JavaScript execution in the OWA origin.
7. Post-exploitation. The script reads Cookie and Authorization headers available to OWA scripts, can call OWA REST endpoints on behalf of the user, can manipulate the DOM to alter the appearance of other messages, and can exfiltrate data to attacker-controlled infrastructure.

2.3 Why Exchange Online Is Not Affected

Exchange Online's OWA codebase has diverged from on-premises since 2020. The specific rendering routine containing the vulnerability does not exist in the cloud variant, which uses a different sanitization pipeline.

2.4 Why CVSS 8.1 Understates the Risk for Targeted Use

The CVSS base score of 8.1 reflects User Interaction Required (the recipient must open the message). For targeted attacks against employees whose role requires opening every inbound message — legal counsel, HR, public-facing roles, executive assistants — that “interaction” is effectively guaranteed. Practitioners should treat this as critical in operational risk terms regardless of the formal score.

3. Detection — Microsoft Defender XDR Advanced Hunting

3.1 Detection Limitations

The vulnerability triggers in the recipient’s browser, not on the Exchange server itself, which means:

- Standard EDR on the recipient endpoint may see browser-initiated outbound connections but will not see the inbound payload that triggered them.
- Exchange server EDR/AV will not flag the message body unless explicitly trained on the payload pattern.
- IIS logs on Exchange Server will show the OWA fetch but not the script execution.

Detection therefore focuses on three layers: inbound message anomalies on Exchange, OWA-originated network activity on endpoints, and Exchange server post-exploitation artifacts.

3.2 KQL Queries

Hunt 1 — Anomalous OWA-originated browser connections

JavaScript executing in OWA will typically initiate fetches to attacker infrastructure for either C2 or data exfiltration. Hunt for browser processes making unexpected outbound connections shortly after an OWA session is active.

```
# let owaSessions = DeviceNetworkEvents
| where Timestamp > ago(7d)
| where RemoteUrl has_any ("outlook.local", "/owa/", "mail.")
| where InitiatingProcessFileName in~ ("msedge.exe", "chrome.exe", "firefox.exe", "iexplore.exe", "brave.exe")
| project SessionTime = Timestamp, DeviceName, BrowserPid = InitiatingProcessId,
    InitiatingProcessFileName, OwaUrl = RemoteUrl;

let suspiciousFetches = DeviceNetworkEvents
| where Timestamp > ago(7d)
| where InitiatingProcessFileName in~ ("msedge.exe", "chrome.exe", "firefox.exe", "iexplore.exe", "brave.exe")
| where RemoteUrl !has_any ("outlook.local", "microsoft.com", "office.com", "office365.com", "msftauth.net", "msauth.net", "windowsupdate.com")
| where RemoteIPType == "Public"
| project FetchTime = Timestamp, DeviceName, BrowserPid = InitiatingProcessId,
    FetchUrl = RemoteUrl, RemoteIP;

owaSessions
| join kind=inner suspiciousFetches on DeviceName, BrowserPid
| where datetime_diff('second', FetchTime, SessionTime) between (0 .. 600)
| project DeviceName, SessionTime, OwaUrl, FetchTime, FetchUrl, RemoteIP
| order by FetchTime desc
```

Hunt 2 — OWA mailbox API access from unusual user-agents

Post-exploitation, the attacker's JavaScript will call OWA REST endpoints to enumerate the mailbox. Anomalous user-agent strings or call patterns on `/owa/service.svc/`, `/owa/sessiondata.ashx`, or `/owa/ev.owa2` are early indicators.

```
DeviceNetworkEvents
| where Timestamp > ago(7d)
| where RemoteUrl has_any ("/owa/service.svc","/owa/sessiondata.ashx","/owa/ev.owa2")
| where InitiatingProcessFileName !in~
("msedge.exe","chrome.exe","firefox.exe","outlook.exe","iexplore.exe")
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine,
RemoteUrl, RemoteIP
| order by Timestamp desc
```

Hunt 3 — Unexpected OAuth or token activity from mailbox accounts

Token theft via OWA XSS will manifest as authentication events from new IP geolocations within minutes of an OWA session. Cross-reference with EntraID sign-in logs.

```
IdentityLogonEvents
| where Timestamp > ago(7d)
| where LogonType == "Interactive" or LogonType == "RemoteInteractive"
| summarize SessionCount = count(),
    DistinctIPs = dcount(IPAddress),
    IPList = make_set(IPAddress, 20),
    Countries = make_set(Location, 10)
    by AccountUpn, bin(Timestamp, 1h)
| where DistinctIPs > 2 or array_length(Countries) > 1
| order by Timestamp desc
```

Hunt 4 — Email messages with suspicious OWA-renderable payloads

Where Defender for Office 365 is licensed, hunt for inbound mail with HTML body characteristics consistent with the published exploitation pattern. This query is a heuristic — tune to your environment.

```
EmailEvents
| where Timestamp > ago(14d)
| where DeliveryAction == "Delivered"
| join kind=inner (
    EmailUrlInfo
    | where Url has_any ("javascript:", "data:text/html", "data:application")
) on NetworkMessageId
| project Timestamp, SenderFromAddress, RecipientEmailAddress, Subject, Url, NetworkMessageId
| order by Timestamp desc
```

Hunt 5 — IIS log anomalies on Exchange Server

For Exchange servers with IIS logs forwarded to Sentinel or another log platform, hunt for OWA requests with unusually large query strings or anomalous referrers from internal addresses.

```
W3CIISLog
| where TimeGenerated > ago(7d)
| where csUriStem has "/owa/"
| where csUriQuery contains "%3C" or csUriQuery contains "%22" or csUriQuery contains
"javascript"
| project TimeGenerated, Computer, slp, clp, csMethod, csUriStem, csUriQuery, csReferer, csUserAgent, scStatus
| order by TimeGenerated desc
```

Hunt 6 — Post-exploitation tooling from Exchange-adjacent endpoints

If credentials are stolen via OWA XSS and reused for lateral movement, the typical follow-on is PowerShell-based mailbox enumeration. Hunt for New-PSSession against Exchange URIs from unusual sources.

```
DeviceNetworkEvents
| where Timestamp > ago(7d)
| where RemoteUrl has_any ("/owa/service.svc","/owa/sessiondata.ashx","/owa/ev.owa2")
| where InitiatingProcessFileName !in~
("msedge.exe","chrome.exe","firefox.exe","outlook.exe","iexplore.exe")
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine,
RemoteUrl, RemoteIP
| order by Timestamp desc
```

4. Mitigation Playbook

4.1 Phase 1 — Verify EMS State (Day 0, immediately)

Goal: Confirm that the automatic mitigation CVE-2026-42897-M2 is active on every Exchange Server in the estate.

Exchange Management Shell:

```
# List all Exchange servers and applied EMS mitigations
Get-ExchangeServer | Get-ExchangeEmergencyMitigation
# Expected output should include:
# MitigationId : CVE-2026-42897-M2
# Status      : Applied
# AppliedDate : <recent timestamp>
# If EMS state cannot be determined, run Health Checker:
# Download from https://aka.ms/ExchangeHealthChecker
.\HealthChecker.ps1 -Server <ExchangeServerName>
```

If CVE-2026-42897-M2 is not Applied:

8. Verify EMS is enabled: `Get-OrganizationConfig | Format-List MitigationsEnabled`. Value should be True.

9. Verify outbound HTTPS to `officecdn.microsoft.com` is permitted from the Exchange server.

10. Force a refresh: `Get-ExchangeServer | ForEach-Object { Get-ExchangeEmergencyMitigation $_.Name }`.

11. Check the Exchange Server event log under Applications and Services → MSExchange Management → EMS for failure events.

4.2 Phase 2 — Manual Mitigation Where EMS Is Unavailable (Day 0—1)

For air-gapped environments or organizations that have explicitly disabled EMS due to internal change-control:

```
# Download EOMT from Microsoft (signed):
# https://github.com/microsoft/CSS-Exchange/releases/latest/download/EOMT.ps1

# Verify Microsoft signature before execution
Get-AuthenticodeSignature .\EOMT.ps1

# Apply CVE-specific mitigation on a single server:
.\EOMT.ps1 -CVE "CVE-2026-42897" -ApplyMitigation

# Apply across all servers in the organization:
Get-ExchangeServer | ForEach-Object {
    Invoke-Command -ComputerName $_.Name -ScriptBlock {
        & "C:\Path\To\EOMT.ps1" -CVE "CVE-2026-42897" -ApplyMitigation
    }
}
# Verify after run:
Get-ExchangeServer | Get-ExchangeEmergencyMitigation | Where-Object {
    $_.MitigationId -eq "CVE-2026-42897-M2"
} | Out-Null
```

4.3 Phase 3 — Compensating Controls Around OWA (Day 1—7)

These controls reduce blast radius if the mitigation is bypassed or if a related variant emerges before a full patch ships.

Conditional Access

Policy	Setting
Target Cloud App	Exchange Online (also affects on-prem with hybrid modern auth)
Users	All users, with break-glass exclusion
Conditions: Client App	Browser
Grant Controls	Require MFA + Require Compliant Device (Intune-managed)
Session Controls	Sign-in frequency 1 hour, persistent browser sessions disabled

For environments still using legacy authentication on OWA, prioritize moving to Modern Authentication. Legacy Basic Auth on OWA is structurally incompatible with the mitigation strategy here.

Web Application Firewall (where deployed)

- Inspect inbound OWA traffic for the exploitation pattern. SOC Prime, Snort/Suricata community rules, and major WAF vendors are publishing signatures for CVE-2026-42897.
-
- Rate-limit OWA endpoints to slow automated scanning.
-
- Enforce strict Content-Security-Policy headers on OWA (may have functional side effects — test before production rollout).

Network Segmentation

OWA should not have unrestricted lateral access to domain controllers, file shares, or backup infrastructure. If your Exchange Servers are not segmented, this incident is the business case for the budget request.

Outbound from Exchange Servers to internet should be restricted to Microsoft endpoints only.

4.4 Phase 4 — Operational Workarounds for Known Side Effects

The EMS mitigation has documented functional impact. Communicate these to OWA users proactively:

Affected feature	Workaround
OWA Print Calendar	Export calendar to .ics, or use Outlook desktop client to print
Inline images in OWA reading pane	Sender should attach images rather than inline
OWA Light (deprecated component)	No workaround. Component is not intended for production use.

4.5 Phase 5 — High-Risk User Hardening (Day 1–14)

- For executive leadership, legal, finance, and other high-value roles, layer additional controls:
- Restrict external OWA access via Conditional Access "compliant device" or "trusted network location" requirements until the permanent patch ships.
- Enable Defender for Office 365 Safe Links and Safe Attachments with Strict preset for these users.
- Run targeted phishing simulations with payloads that mimic the public CVE-2026-42897 indicators to validate that detection and user-awareness controls trigger as expected.
- Audit OAuth application consent grants for these mailboxes — XSS-derived tokens are often used to grant persistent third-party app access.

5. PowerShell — Operational Verification Scripts

5.1 Health Check Script (Run Daily Until Patch Ships)

```
# CVE-2026-42897 health check
# Run on each Exchange Server or remotely with appropriate RBAC
$results = Get-ExchangeServer | ForEach-Object {
    $server = $_.Name
    try {
        $mitigations = Get-ExchangeEmergencyMitigation -Identity $server -ErrorAction Stop
        $cveMitigation = $mitigations | Where-Object { $_.MitigationId -eq "CVE-2026-42897-M2" }
        [PSCustomObject]@{
            Server          = $server
            EMSEnabled     = ($mitigations.Count -gt 0)
            CVE42897Applied = ($null -ne $cveMitigation -and $cveMitigation.Status -eq "Applied")
            AppliedDate    = $cveMitigation.AppliedDate
            CheckTime      = Get-Date
        }
    }
    catch {
        [PSCustomObject]@{
            Server          = $server
            EMSEnabled     = $false
            CVE42897Applied = $false
            AppliedDate    = $null
            CheckTime      = Get-Date
            Error           = $_.Exception.Message
        }
    }
}
$results | Format-Table -AutoSize
if ($results | Where-Object { -not $_.CVE42897Applied }) {
    Write-Warning "One or more Exchange Servers are not protected against CVE-2026-42897."
    exit 1
} else {
    Write-Output "All Exchange Servers have CVE-2026-42897-M2 applied."
    exit 0
}
```

5.2 OWA Endpoint Reachability Audit

```
# Identify which OWA endpoints are reachable from the public internet
$exchangeServers = Get-ExchangeServer | Where-Object { $_.IsClientAccessServer -eq $true }
$externalUrls = $exchangeServers | ForEach-Object {
    $vd = Get-OwaVirtualDirectory -Server $_.Name -ADPropertiesOnly
    [PSCustomObject]@{
        Server      = $_.Name
        ExternalUrl = $vd.ExternalUrl
        InternalUrl = $vd.InternalUrl
    }
}
$externalUrls | Format-Table -AutoSize
```

6. CIS Critical Security Controls v8 — Mapping

6.1 Directly affected controls

Control	IG	Status	Implication
7.1 Establish Vulnerability Management Process	IG1	Process exercised	EMS-driven mitigation is the operational manifestation of "continuous management"
7.2 Establish Remediation Process	IG1	Process exercised	Documented timeline from disclosure to mitigation to expected patch
7.4 Automated Application Patch Management	IG1	Insufficient alone	Patching alone leaves a window — see this advisory's premise
7.7 Remediate Detected Vulnerabilities	IG2	In progress	Mitigation applied; permanent remediation pending Microsoft patch
4.1 Secure Configuration Process	IG1	Baseline update needed	OWA hardening (CSP, header policy, modern auth) should be in baseline
6.3 MFA for Externally-Exposed Apps	IG1	Reinforcement	If OWA is internet-facing without MFA, this incident is the trigger to fix
6.4 MFA for Remote Network Access	IG1	Reinforcement	Conditional Access on OWA falls under this
8.2 Collect Audit Logs	IG1	Operational	IIS, OWA, EntraID sign-in logs must be retained and queryable
13.1 Centralize Security Event Alerting	IG2	Operational	Hunts in section 3 require centralized logs
13.6 Collect Network Traffic Flow Logs	IG2	Operational	OWA outbound from endpoints requires net-flow visibility

6.2 Recommended Master Baseline Policy Updates

IG1 (minimum baseline)

- Exchange Server EMS state monitored as part of standard server inventory.
- OWA external access requires MFA via Conditional Access (where ExchangeOnline-equivalent control is feasible).
- Quarterly verification that EMS feed connectivity (officecdn.microsoft.com) is permitted on all Exchange Servers.

IG2 (recommended for most organizations)

- All KQL hunts from section 3 deployed as scheduled detections in Defender XDR.
- Conditional Access policies for OWA include device compliance check.
- WAF inspection of OWA traffic with signature updates from at least one commercial threat intelligence feed.
- Documented procedure for forced manual mitigation via EOMT for any server where EMS feed is unavailable.

IG3 (high security)

- OWA external exposure removed entirely; remote access to mailbox via VPN or Cloud-based Exchange Online only.
- Continuous validation of EMS state via SOAR — any server reporting CVE-2026-42897-M2 as not Applied triggers an automated incident.
- Behavioral baselining of OWA usage per user, with anomaly detection on session geolocation and inter-session intervals.

6.3 Mapping to Other Frameworks

NSM Grunnprinsipper for IKT-sikkerhet 2.0

- 2.3.1 (Beskytt enheter og programvare) — directly invoked; Exchange Server is the affected device class
- 2.4.1 (Beskytt data i bevegelse) — OWA traffic protection via TLS and WAF
- 3.3.4 (Analyser data fra sikkerhetsovervåking) — detection hunts in section 3
- 4.1.1 (Forbered virksomheten på hendelser) — incident-response readiness for confirmed exploitation

NIST Cybersecurity Framework 2.0

- ID.RA-01 (Vulnerabilities in assets are identified) — vulnerability inventory must include EMS state
- PR.PS-02 (Software is maintained, replaced, and removed) — mitigation as interim control while awaiting patch
- DE.CM-01 (Networks and network services are monitored) — KQL hunts cover this
- RS.MI-02 (Newly identified vulnerabilities are mitigated) — EMS is the operational embodiment of this

ISO 27001:2022 Annex A

- A.8.8 (Management of technical vulnerabilities) — process exercised
- A.8.9 (Configuration management) — baseline updated to require EMS-enabled state
- A.8.16 (Monitoring activities) — detection hunts deployed

7. Timeline and Follow-up

Date	Event
13 May 2026	Microsoft Patch Tuesday — 118 CVEs, no actively exploited such release since June 2024.
14 May 2026	Microsoft discloses CVE-2026-42897. Confirms active exploit. Publishes EMS mitigation CVE-2026-42897-M2.
15 May 2026	CISA adds CVE-2026-42897 to Known Exploited Vulnerability (KEV) database. FCEB deadline: 29 May 2026.
17 May 2026	This advisory issued.
Late May / June 2026 (expected)	Microsoft releases security update. CVE may be addressed Patch Tuesday or earlier out-of-band.
Post-patch	This advisory will be revised; EMS mitigation can be removed once permanent patch is verified applied.

Centrio and nLogic monitor Microsoft's response and will revise this advisory upon patch release or new exploitation.

8. References

Microsoft Community Hub — Addressing Exchange Server May 2026 vulnerability CVE-2026-42897 — <https://techcommunity.microsoft.com/blog/exchange/addressing-exchange-server-may-2026-vulnerability-cve-2026-42897/4518498>

Microsoft Security Update Guide — CVE-2026-42897
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897>

CISA Known Exploited Vulnerabilities Catalog
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

NVD — CVE-2026-42897
<https://nvd.nist.gov/vuln/detail/CVE-2026-42897>

The Hacker News On-Prem Microsoft Exchange Server CVE-2026-42897 Exploited via Crafted Email
<https://thehackernews.com/2026/05/on-prem-microsoft-exchange-server-cve.html>

BleepingComputer Microsoft warns of Exchange zero-day flaw exploited in attacks
<https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-exchange-zero-day-flaw-exploited-in-attacks/>

Help Net Security Unpatched Microsoft Exchange Server vulnerability exploited
<https://www.helpnetsecurity.com/2026/05/15/exchange-server-cve-2026-42897-exploited/>

Security Affairs — Microsoft confirms active exploitation of Exchange Server zero-day
<https://securityaffairs.com/192204/security/cve-2026-42897-microsoft-confirms-active-exploitation-of-exchange-server-zero-day.html>

SOC Prime CVE-2026-42897 Analysis
<https://socprime.com/blog/cve-2026-42897-analysis/>

Microsoft Learn Exchange Server Emergency Mitigation (EM) Service
<https://learn.microsoft.com/en-us/exchange/exchange-emergency-mitigation-service-exchange-server>

Microsoft CSS-Exchange Exchange On-premises Mitigation Tool (EOMT)
<https://github.com/microsoft/CSS-Exchange>

Exchange Health Checker
<https://aka.ms/ExchangeHealthChecker>

BleepingComputer Microsoft May 2026 Patch Tuesday fixes 120 flaws, no zero-days
<https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2026-patch-tuesday-fixes-120-flaws-no-zero-days/>

CIS Critical Security Controls v8
<https://www.cisecurity.org/controls/v8>

NSM Grunnprinsipper for IKT-sikkerhet 2.0
<https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/>

NIST Cybersecurity Framework 2.0
<https://www.nist.gov/cyberframework>

7. About nLogic

nLogic AS is a trusted Nordic partner for high-performance network and security solutions. We help organizations secure critical infrastructure through architectures grounded in Zero Trust principles, the CIS Critical Security Controls, NSM's Basic Principles for ICT Security, and the NIST Cybersecurity Framework.

This advisory was prepared by Kim Hansen, Security Advisor, nLogic AS. For tailored guidance on applying these recommendations to your environment, please contact your nLogic representative.

Disclaimer

This document is an advisory, not a legal or compliance statement. Configuration changes to Exchange Server, EMS, or surrounding security controls must be validated against the organization's own risk profile, change-control procedures, and operational readiness before production deployment. Centrio AS and nLogic AS disclaim liability for application of this guidance outside an engagement-specific scope of work.



Concerned about your current security posture and potential risks? Contact nLogic for an initial conversation.

Thomas Brodersen, IT Security Advisor, nLogic
thomas.brodersen@nlogic.no
+47 958 30 108