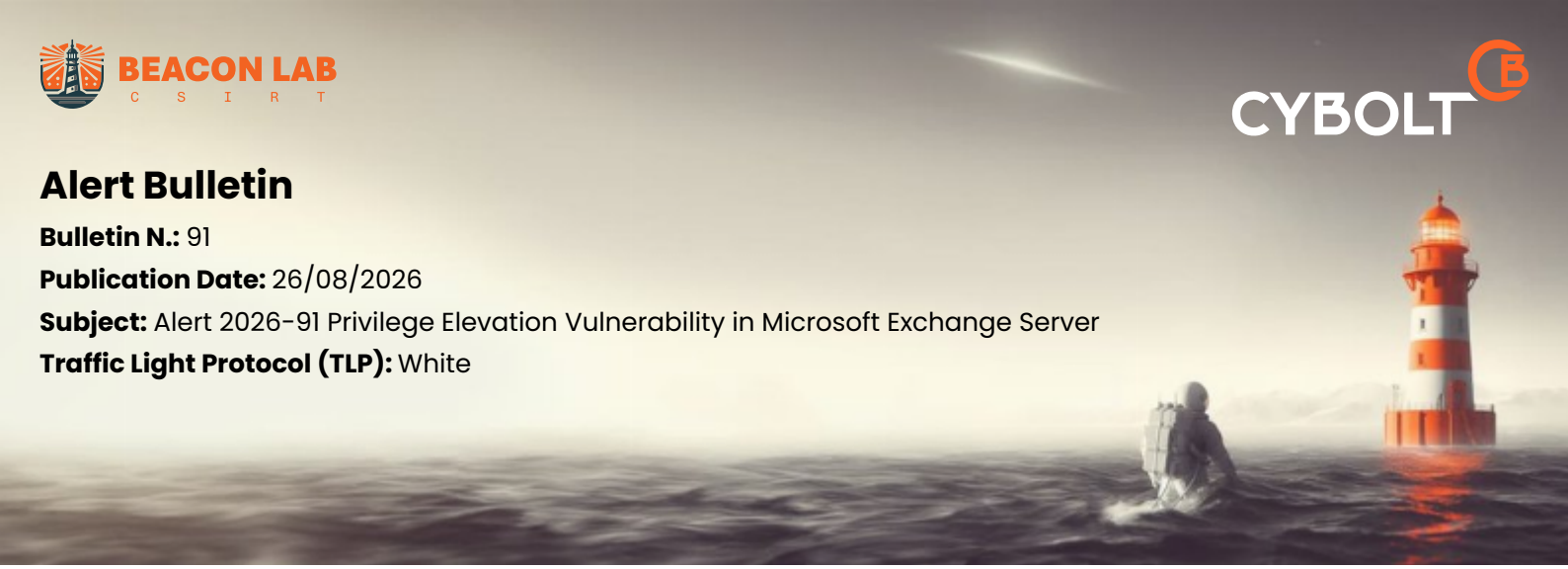

Alert Bulletin

Bulletin N.: 91
Publication Date: 26/08/2026
Subject: Alert 2026-91 Privilege Elevation Vulnerability in Microsoft Exchange Server
Traffic Light Protocol (TLP): White

Affected product(s):

- Microsoft Exchange Server 2016 CU23 (x64): versions from 15.01.0.0 up to before **15.01.2507.072**.
- Microsoft Exchange Server 2019 CU14 (x64): versions from 15.02.0.0 up to before **15.02.1544.044**.
- Microsoft Exchange Server 2019 CU15 (x64): versions from 15.02.0.0 up to before **15.02.1748.049**.
- Microsoft Exchange Server Subscription Edition (SE) RTM (x64): versions from 15.02.0.0 up to before **15.02.2562.046**.

Description

Recently, Microsoft disclosed vulnerability CVE-2026-62911, reported by Orange Tsai from the DEVCORE Research Team, in Microsoft Exchange Server, an on-premises email, calendar, and enterprise collaboration platform. The vulnerability has high severity, with a CVSS v3.1 score of 8.0 and may allow an authenticated attacker with low privileges to elevate their permissions over the network.

The vulnerability is classified as CWE-294: Authentication Bypass by Capture-Replay. An attacker can reuse a previously captured request or authentication material to bypass intended authentication controls, enabling access with higher privileges within Exchange.

The analysis published by Zero Day Initiative indicates that the issue resides in the processing of authorization requests and in inadequate session management. In an exploitation scenario, this condition can be chained with other vulnerabilities to achieve code execution under the SYSTEM context, compromising the confidentiality, integrity, and availability of the server.

There is no public evidence of active exploitation at the time of publication. However, CISA classifies the potential technical impact as total; therefore, exposed or high-criticality Exchange servers should be prioritized in the patching cycle.

Solution:

Microsoft fixed the vulnerability through the security updates published in **August 2026**. It is recommended to immediately apply the corresponding Security Update and verify that the server reaches, at minimum, the corrected builds indicated above.

For Exchange Server 2019 CU15, install KB5121574. For Exchange Server 2016 CU23, install KB5121576. Updates for Exchange SE and Exchange 2019 CU14 are available in the August 2026 Security Updates bulletin.

Exchange Server 2016 and 2019 are already out of general support; the August 2026 updates require enrollment in the Extended Security Updates (ESU) program, period 2. Organizations that do not have ESU should plan the migration to Exchange Server Subscription Edition. After updating, it is recommended to run the Exchange Server Health Checker to validate the installation and review additional configurations.

As exposure reduction measures, limit access to Exchange only to necessary networks and users, apply least privilege to accounts, monitor anomalous authentication and authorization events, and analyze repeated requests or unusual sessions.

Additional information:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911
- https://www.zerodayinitiative.com/advisories/ZDI-26-538/
- https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates