NATIONAL CSIRT-CY

Critical Privilege Escalation Vulnerability in **ASP.NET Core**

22 April 2026

[Cyber Threat Intelligence]

EXECUTIVE SUMMARY:

The Digital Security Authority (DSA) has observed Microsoft has released out-of-band security updates to remediate a critical vulnerability (CVE-2026-40372) affecting **ASP.NET Core**. The flaw, with a CVSS score of 9.1, enables remote privilege escalation to SYSTEM level due to improper cryptographic signature validation.

TECHNICAL DETAILS:

Microsoft has released out-of-band security updates to remediate a critical vulnerability (CVE-2026-40372) affecting ASP.NET Core. The flaw, with a CVSS score of 9.1, enables remote privilege escalation to SYSTEM level due to improper cryptographic signature validation.

The issue specifically impacts applications using vulnerable versions of the Data Protection component distributed via NuGet. Exploitation could allow attackers to forge authentication tokens, access sensitive data, and maintain persistent access even after patching unless additional remediation steps are taken.

Vulnerability Details

- CVE ID: CVE-2026-40372
- Severity: **9.1 CRITICAL**
- Impact: Privilege Escalation, Authentication Bypass, Data Disclosure
- Affected Component: Microsoft.AspNetCore.DataProtection (v10.0.0 – v10.0.6)
- Fixed Version: 10.0.7

Weakness Enumerations

- CWE-347 Improper Verification of Cryptographic Signature

RECOMMENDATIONS:

Update Immediately: Microsoft.AspNetCore to fixed version or later.

Rotate Data Protection Key Ring

- Invalidate all previously issued cryptographic tokens
- This is essential to neutralize forged tokens generated during the vulnerable window

Please ensure to distribute this information among your subsidiaries and partners and provide us with any pertinent information or findings you may have (such as Indicators of Compromise, Tactics, Techniques, and Procedures, etc.).

The Digital Security Authority (DSA) extends its appreciation for the continued collaboration.

REFERENCES:

1. https://nvd.nist.gov/vuln/detail/CVE-2026-40372

DISCLAIMER:

The information presented in this report is based on available data up to the 22nd of April 2026.

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.