Secure Halo Urges Organizations to Act on Critical Microsoft ASP.NET Core Vulnerability

May 07, 2026

SILVER SPRING, MD - May 07, 2026 - PRESSADVANTAGE -

Secure Halo, a cybersecurity services firm based in Silver Spring, Maryland, is urging organizations running applications built on Microsoft's ASP.NET Core framework to take immediate action following the disclosure of a critical security vulnerability affecting the platform. The vulnerability, tracked as CVE-2026-40372, was assigned a severity rating of 9.1 out of 10 and affects versions 10.0.0 through 10.0.6 of the Microsoft.AspNetCore.DataProtection NuGet package.

Microsoft issued an emergency patch on April 22, 2026, after discovering a regression bug in the package that allowed the managed authenticated encryptor to compute its HMAC validation tag over incorrect payload bytes. The flaw stems from a faulty verification of cryptographic signatures and can be exploited to allow unauthenticated attackers to forge authentication payloads during the HMAC validation process, a mechanism used to verify the integrity and authenticity of data exchanged between a client and a server. Successful exploitation could allow an unauthenticated attacker to gain SYSTEM-level privileges on affected Linux and macOS devices, resulting in full compromise of the underlying machine.

"This vulnerability is particularly concerning because patching alone does not close the exposure window,"

said Matt Yates at Secure Halo. "Any organization that was running a vulnerable version on an internet-exposed endpoint needs to treat this as an active incident response situation, not simply a routine update. Rotating the DataProtection key ring and auditing application-level artifacts are required steps, and many organizations may not have the internal resources or processes to execute that effectively under time pressure."

Microsoft has advised that affected users are primarily those who ran version 10.0.6 at runtime on macOS, Linux, or other non-Windows operating systems. Windows applications are not affected because DataProtection defaults to encryptors that do not contain the underlying bug. However, the remediation process extends beyond the installation of the 10.0.7 patch. Organizations that served internet-exposed endpoints while running a vulnerable version must rotate their DataProtection key ring to address the possibility that forged credentials were introduced during the exposure window.

Of particular concern to security professionals is the persistence of forged authentication artifacts beyond the patch itself. According to Microsoft, if an attacker used forged payloads to authenticate as a privileged user during the vulnerable period, the application may have issued legitimately signed tokens, including session refresh tokens, API keys, and password reset links, to the attacker. Those tokens remain valid after upgrading to version 10.0.7 unless the key ring is rotated and application-level artifacts are reviewed and invalidated.

Secure Halo noted that this type of vulnerability illustrates a broader challenge organizations face in maintaining visibility into the full scope of their software dependencies and the downstream risk those dependencies carry. The Microsoft.AspNetCore.DataProtection package is widely used across web application development environments, and the speed with which the vulnerability moved from disclosure to emergency patch reflects the severity of the underlying risk.

The firm provides a range of cybersecurity services relevant to situations of this nature, including managed detection and response, penetration testing, cybersecurity assessments, and virtual Chief Information Security Officer engagements. Secure Halo has worked with organizations across sectors including finance, healthcare, government, insurance, manufacturing, and utilities, and has developed security programs for clients that include response procedures for newly disclosed vulnerabilities and rapid patch management protocols.

Organizations that are uncertain whether their applications were affected by CVE-2026-40372 are encouraged to review Microsoft's published guidance, which includes detailed instructions for assessing exposure, rotating keys, and auditing artifacts that may have been created during the vulnerable window. Secure Halo has indicated that its team is available to assist organizations in evaluating their exposure and developing a structured remediation plan.

For more information about Secure Halo's cybersecurity services and how the firm assists organizations in responding to emerging threats, visit Secure Halo.

###

For more information about Secure Halo, contact the company here:Secure HaloErin Webb202-629-1960info@securehalo.com962 Wayne Ave, Suite 310, Silver Spring, MD 20910


```
{
  "@context": "https://schema.org",
  "@type": "Organization",
  "name": "Secure Halo",
  "url": "https://securehalo.com/",
  "logo": "https://securehalo.com/wp-content/uploads/2025/01/securehalo-logo.png",
  "contactPoint": [
    {
      "@type": "ContactPoint",
      "telephone": "+1-202-629-1960",
      "contactType": "Customer Service",
      "email": "info@securehalo.com",
      "areaServed": "US"
    },
    {
      "@type": "ContactPoint",
      "telephone": "+1-301-304-1700",
      "contactType": "Sales",
      "email": "info@securehalo.com",
      "areaServed": "US"
    }
  ],
  "address": {
    "@type": "PostalAddress",
    "streetAddress": "962 Wayne Ave, Suite 310",
    "addressLocality": "Silver Spring",
    "addressRegion": "MD",
    "postalCode": "20910",
    "addressCountry": "US"
  },
```

```
  "sameAs": [
    "https://www.linkedin.com/company/secure-halo/",
    "https://twitter.com/SecureHalo",
    "https://www.facebook.com/SecureHalo",
    "https://www.youtube.com/@SecureHalo"
  ],
  "foundingDate": "2002-01-01",
  "founder": {
    "@type": "Person",
    "name": "Secure Halo Leadership Team"
  },
  "parentOrganization": {
    "@type": "Organization",
    "name": "Mission Critical Partners"
  },
    "description": "Secure Halo provides trusted, proactive cybersecurity solutions to protect organizations? data, infrastructure, and business continuity. With expertise across industries including government, healthcare, finance, manufacturing, and utilities, Secure Halo offers services such as vCISO, cybersecurity assessments, managed detection and response, compliance support, penetration testing, insider threat management, and third-party risk management, and third-party risk management."
}
```


Secure Halo

Secure Halo delivers trusted, proactive cybersecurity solutions?protecting data, infrastructure, and business continuity through services like vCISO, assessments, MDR, compliance, penetration testing, insider threat, and third-party risk management.

Website: https://www.securehalo.com/

Email: info@securehalo.com

Phone: 202-629-1960

SECURE HALO

SECURING THE ENTERPRISE

A **Mission Critical Partners** Company