Threat Update Service* Advisory

Protection Pack 2015-05-01-01 Released May 01, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HTTP.sys Remote Code Execution Vulnerability.

Issue: An integer overflow in the IIS caching allows an attacker to read uninitialized memory or cause a "Blue Screen Of Death" (aka BSOD). If an attacker can ensure that the non-paged pool has ~4GB of contiguous memory allocated after the attacker's buffer in IIS, they can potentially read all that data back (although the IIS socket might not allow an attacker to send that much data).

Recommended Action: Apply the specified Protection Pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2015-1635
Advisory	https://technet.microsoft.com/library/security/ms15-034
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to read uninitialized memory or cause a BSOD.
Affected Products	IIS in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-025332
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

