Threat Update Service* Advisory

Protection Pack 2015-01-19-02 Released January 19, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Windows CVE-2015-0016 Remote Privilege Escalation Vulnerability.

Issue: Microsoft Windows TSWebProxy Active-X control allows running of arbitrary executables. This could allow an attacker to execute arbitrary code on the victim's machine by elevating privileges and enticing the victim to open a specially crafted file. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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-2015-0016, MS15-004
Advisory	https://technet.microsoft.com/library/security/ms15-004
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.82 (build 003 and later).
Associated Rule	tln-107010
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

