Threat Update Service* Advisory

Protection Pack 2015-02-13-01 Released February 13, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Windows Win32k.sys CVE-2015-0059 Remote Code Execution Vulnerability.

Issue: Microsoft Windows kernel is prone to a remote code-execution vulnerability. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted TrueType font. 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-2015-0059, MS15-010
Advisory	https://technet.microsoft.com/library/security/ms15-010
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows 8.1 Microsoft Windows RT Microsoft Windows RT 8.1 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2012 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-107044
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

