Threat Update Service* Advisory

Protection Pack 2014-12-11-02 Released December 12, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Exchange Server CVE-2014-6325 Security Bypass Vulnerability.

Issue: Microsoft Exchange Server does not properly handle malicious JavaScript elements within a specially crafted URL which can lead to a cross-site scripting attack. This could allow an attacker to get elevated privileges or execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website. 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-2014-6325, MS14-075
Advisory	https://technet.microsoft.com/library/security/ms14-080
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 Exchange Server 2013 SP1
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-107006
Associated Rule Set	This rule has to be enabled manually.

* previously called TopResponse

