

Threat Update Service* Advisory

Protection Pack 2013-10-06-01 Released October 6, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Office CVE-2013-3155 Access Database Processing Pointers Vulnerability.

Issue: Microsoft Access improperly accesses memory when parsing Access files thereby corrupting system memory. This could allow an attacker to execute arbitrary code on the victim's machine by 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-2013-3155, MS13-074
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-074
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Microsoft Access 2007 SP3, 2010 SP1 and SP2, and 2013
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-022182
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA Copyright 2013. All Rights Reserved.