Threat Update Service* Advisory

Protection Pack 2013-12-13-01 Released December 13, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft nVerifyTrust CVE-2013-3900 Signature Validation Vulnerability.

Issue: The WinVerifyTrust function does not properly validate the file digest of PE files while verifying the Windows Authenticode signature. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted PE 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-2013-3900, MS13-098
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-098
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Windows XP Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows 8 and Windows 8.1 Windows 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1
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-509013
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