Threat Update Service* Advisory

Protection Pack 2013-11-01-03 Released November 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the WellinTech KingView ActiveX Controls Multiple Insecure Method Vulnerability.

Issue: The SUPERGRIDLib.SuperGrid and KCHARTXYLib.KChartXY ActiveX controls in WellinTech KingView do not properly restrict calls to ReplaceDBFile and SaveToFile methods respectively. This could allow a remote attacker to execute arbitrary code on the vulnerable machine via a directory traversal attack. An attacker who successfully exploited this vulnerability could possibly 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-2013-6127, CVE-2013-6128
Advisory	http://ics-cert.us-cert.gov/advisories/ICSA-13-295-01
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	WellinTech KingView before 6.53
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-106732
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