Threat Update Service* Advisory

Protection Pack 2012-10-26-04 Released October 26, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the GE Proficy Historian KeyHelp.ocx ActiveX Remote Code Execution Vulnerability.

Issue: A command injection vulnerability exists in an ActiveX control in KeyHelp.ocx in the KeyWorks KeyHelp Module. This could allow an attacker to execute arbitrary code on the remote machine by sending specially crafted input. 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-2012-2516
Vendor Advisory	http://support.ge-ip.com/support/resources/sites/GE_FANUC_SUPPORT/content/live/KB/14000/KB14863/en_US/GEIP12-04%20Security%20Advisory%20-%20Proficy%20HTML%20Help.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	GE Intelligent Platforms Proficy Historian 3.1, 3.5, 4.0, and 4.5 Proficy HMI/SCADA iFIX 5.0 and 5.1 Proficy Pulse 1.0 Proficy Batch Execution 5.6 SI7 I/O Driver 7.20 through 7.42
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025144
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