Threat Update Service* Advisory

Protection Pack 2014-03-06-01 Released March 6, 2014

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

Issue: A directory traversal vulnerability exists in gefebt.exe in the WebView CimWeb components in GE Intelligent Platforms Proficy. This could allow an attacker to execute arbitrary code on the affected system via a specially crafted HTTP request.

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-2014-0750
Advisory	http://support.ge-ip.com/support/index?page=kbchannel&id=KB15939
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	GE Intelligent Platforms Proficy HMI/SCADA - CIMPLICITY through 8.2 SIM 24 Proficy Process Systems with CIMPLICITY
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-025242
Associated Rule Set	This rule is automatically enabled in the “Strict Server 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