Threat Update Service* Advisory

Protection Pack 2012-10-05-02 Released October 5, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP Application Lifecycle Management xgo.ocx Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the XGO.ocx ActiveX Control in HP Application Lifecycle Manager. This could allow an attacker to execute arbitrary code on the remote machine by sending specially crafted paramters to the SetShapeNodeType method. 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	BID: 55272
Advisory	http://www.securityfocus.com/bid/55272/info
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	HP Application Lifecycle Manager 11.50
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025140
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