Threat Update Service* Advisory

Protection Pack 2013-04-01-03 Released April 1, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Mitsubishi MX ActiveX Component ActUWzd.dll Heap Spray Vulnerability.

Issue: A remote buffer overflow vulnerability exists in the ActUWzd.dll ActiveX control in Mitsubishi MX. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system by enticing the victim to open a specially crafted website.

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: 58692
Advisory	http://www.securityfocus.com/bid/58692/discuss
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Mitsubishi MX
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106605
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

