Threat Update Service* Advisory

Protection Pack 2012-08-31-02 Released August 31, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle AutoVue ActiveX Control SetMarkupMode Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the SetMarkupMode method in the AutoVue.ocx ActiveX control. This could allow an attacker to execute arbitrary code on the remote machine by enticing the user to open a specially crafted website. 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-2012-0549
Vendor Advisory	http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Oracle AutoVue Desktop v20.1.1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025138
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

