Threat Update Service* Advisory

Protection Pack 2014-07-03-01 Released July 3, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Ericom AccessNow Server CVE-2014-3913 Stack Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in AccessServer32.exe in Ericom AccessNow Server. This could allow an attacker to execute arbitrary code on the victim's machine via a request for an non-existent file. 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-2014-3913
Advisory	http://www.ericom.com/security-ERM-2014-610.asp
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Ericom AccessNow Server
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-025263
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

