Threat Update Service* Advisory

Protection Pack 2014-01-23-01 Released January 23, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Multiple Routers Remote Code Execution Vulnerability.

Issue: Multiple routers contain undocumented backdoor services that can be exploited by an attacker to execute arbitrary code on the machine via a specially crafted packet. This could allow the attacker to possibly take complete control of the 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: 64675
Advisory	http://www.securityfocus.com/bid/64675/info
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	SerComm, Netgear and Linksys routers
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-025229
Associated Rule Set	This rule is automatically enabled in the “Recommended 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