

Threat Update Service* Advisory

Protection Pack 2014-01-08-02 Released January 9, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the D-Link RuntimeDiagnosticPing Stack Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the RuntimeDiagnosticPing function in D-Link DIR-100 routers. This could allow an attacker to execute arbitrary commands on the victim's machine via a long set/runtime/diagnostic/pinglp parameter to Tools/tools_misc.xg.

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-2013-6027
Advisory	http://www.kb.cert.org/vuls/id/248083
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary commands on an unprotected system.
Affected Products	D-Link DIR-100 routers
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106763
Associated Rule Set	This rule is automatically enabled in the "Strict 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
• USA • Japan • Asia Pacific • EMEA Copyright 2014. All Rights Reserved.