

Threat Update Service* Advisory
Protection Pack 2013-10-06-01 Released October 6, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the D-Link Devices UPnP SOAP Telnetd Command Execution Vulnerability.

Issue: A command injection vulnerability exists in multiple D-Link devices that could allow an attacker to execute arbitrary code on the system and potentially take complete control of the device as it does not properly sanitize input.

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: 61005
Advisory	http://www.securityfocus.com/bid/61005/discuss
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	DIR-300 rev B running firmware 2.14b01 DIR-600 running firmware 2.16b01 DIR-645 running firmware 1.04b01 DIR-845 running firmware 1.01b02 DIR-865 running firmware 1.05b03
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-025202
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

• USA • Japan • Asia Pacific • EMEA Copyright 2013. All Rights Reserved.