

Threat Update Service* Advisory

Protection Pack 2012-10-19-02 Released October 19, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP StorageWorks P4000 Virtual SAN Appliance Command Execution Vulnerability.

Issue: hydra.exe in HP SAN/iQ on the HP Virtual SAN Appliance contains a default hardcoded password. This could allow a remote attacker to gain unauthorized access to the management service. 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-2012-4362
Advisory	http://www.kb.cert.org/vuls/id/441363
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	HP SAN/iQ before 9.5 on the HP Virtual SAN Appliance
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106526
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 2012. All Rights Reserved.