

Threat Update Service* Advisory

Protection Pack 2012-08-31-02 Released August 31, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP OpenView Storage Data Protector EXEC_CMD Buffer Overflow Vulnerability.

Issue: A buffer overflow exists in the inet service in HP OpenView Storage Data Protector. This could allow an attacker to execute arbitrary code on the remote machine. 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-2011-1866
Vendor Advisory	http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02872182
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 OpenView Storage Data Protector 6.00 through 6.20
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tIn-022151
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.