Threat Update Service* Advisory

Protection Pack 2014-03-27-01 Released March 28, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP Data Protector Backup Client EXEC_BAR Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the backup client service (OmniInet.exe) in HP Storage Data Protector. This could allow an attacker to execute arbitrary commands on the victim's machine via a crafted EXEC_BAR packet to TCP port 5555.

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-2013-2347
Advisory	http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c03822422
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary commands on an unprotected system.
Affected Products	HP Storage Data Protector 6.2X
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-025246
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

