Threat Update Service* Advisory

Protection Pack 2014-09-26-01 Released September 26, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the GNU Bash CVE-2014-6277 Remote Code Execution Vulnerability.

Issue: Bash does not properly parse function definitions in the values of environment variables. This could allow an attacker to execute arbitrary commands on the victim's machine via a specially crafted request.

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-2014-6277
Advisory	http://www.securityfocus.com/bid/70165
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	GNU Bash through 4.3
Corero Products	IPS / DDS 5500 EC-Series and IPS / DDS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (DDS build 044 and earlier, IPS build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-106933
Associated Rule Set	This rule needs to be enabled and configured.

* previously called TopResponse

http://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