Threat Update Service* Advisory

Protection Pack 2012-12-28-04 Released December 28, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP Data Protector DtbClsLogin Utf8cpy Remote Code Execution Vulnerability.

Issue: A stack buffer overflow vulnerability exists in HP Data Protector. This could allow an attacker to execute arbitrary code on the victim's machine by sending a very long username during the login process. 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-2010-3007
Advisory	http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02498535
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 Data Protector Express HP Data Protector Express Single Server Edition (SSE) 3.x before build 56936 HP Data Protector Express Single Server Edition (SSE) 4.x before build 56906
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025154
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