

Threat Update Service* Advisory
Protection Pack 2013-10-21-01 Released October 21, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Imperva SecureSphere Operations Manager Multiple Security Vulnerabilities.

Issue: Imperva SecureSphere does not properly validate user supplied input to the public and private key parameters in a T/keyManagement request. This could allow an attacker to upload arbitrary files to an affected system and thereafter execute them.

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-2013-4094
Advisory	http://www.securityfocus.com/bid/61065/discuss
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files to an unprotected system.
Affected Products	Imperva SecureSphere 9.0.0.5
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tIn-106725
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 2013. All Rights Reserved.