

Threat Update Service* Advisory

Protection Pack 2013-02-12-03 Released February 12, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apple QuickTime QTIF File Denial-of-Service Vulnerability.

Issue: A denial of service vulnerability exists in Apple QuickTime. This could allow an attacker to crash the affected application by enticing the victim to open a specially crafted '.qtif' file.

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	BID: 57573
Vendor Advisory	http://www.securityfocus.com/bid/57573/info
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service on an unprotected system.
Affected Products	Apple QuickTime 7.7.3
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106582
Associated Rule Set	This rule is automatically enabled in the "Recommended Client 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.