

Threat Update Service* Advisory
Protection Pack 2013-12-03-01 Released December 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the VICIDIAL manager_send.php SQL Injection and Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the VICIDIAL Contact Center Suite. This could allow an attacker to execute arbitrary code on the affected system 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-2013-4467, CVE-2013-4468
Advisory	http://www.securityfocus.com/bid/63340
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	VICIDIAL 2.7RC1, 2.7 and 2.8-403a
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-025216
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.