

Threat Update Service* Advisory
Protection Pack 2014-04-24-06 Released April 25, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the CA 2E Web Option Unauthenticated Privilege Escalation Vulnerability.

Issue: A session hijacking vulnerability exists in CA 2E Web Option as it accepts a predictable substring of the W2E_SSNID session token instead of the entire token.

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-2014-1219
Advisory	http://www.securityfocus.com/bid/65537
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to hijack sessions.
Affected Products	CA 2E Web Option r8.1.2
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106854
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* 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 Copyright 2014. All Rights Reserved.