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 Supermicro Onboard IPMI Login CGI Buffer Overflow Vulnerability.

Issue: A buffer overflow vulnerability exists in the Supermicro Onboard IPMI. 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-2013-3621
Advisory	http://www.supermicro.com/products/nfo/files/IPMI/CVE_Update.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Supermicro IPMI X9SCL/X9SCM with firmware version SMT_X9_214v5.1 or prior
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	tln-025215
Associated Rule Set	This rule is automatically enabled in the “Strict 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