Threat Update Service* Advisory

Protection Pack 2015-01-09-01 Released January 09, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the ManageEngine Arbitrary File Download Vulnerability.

Issue: A file download vulnerability exists in the CSVServlet or CReportPDFServlet in ManageEngine Netflow Analyzer. This could allow an attacker to download and read arbitrary files.

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-2014-5445
Advisory	https://support.zoho.com/portal/manageengine/helpcenter/articles/cve-2014-5445-cve-2014-5446-fix-for-arbitrary-file-download
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to download arbitrary files to an unprotected system.
Affected Products	ManageEngine Netflow Analyzer 8.6 through 10.2
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-107008
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

