

Threat Update Service* Advisory Protection Pack 2014-12-04-04 Released December 5, 2014

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

Issue: An information disclosure vulnerability exists in the ReadUsersFromMasterServlet in ManageEngine DeviceExpert. This could allow an attacker to obtain user account credentials via a direct 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-2014-5377
Advisory	http://www.manageengine.com/products/device-expert/release-notes.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information on an unprotected system.
Affected Products	ManageEngine DeviceExpert before 5.9 build 5981
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	tIn-106988
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* previously called TopResponse