

Threat Update Service* Advisory
Protection Pack 2013-08-30-02 Released August 30, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the HP LoadRunner IrFileIOService ActiveX Control WriteFileBinary Vulnerability.

Issue: A remote code execution vulnerability exists in HP LoadRunner. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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-2013-2370
Advisory	https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03862772
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	HP LoadRunner before 11.52
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	tlIn-022177
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse