



CVE-2014-2610

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-2610
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-19 10:50:00 UTC
Updated	2014-06-26 04:49:00 UTC
Description	Directory traversal vulnerability in the Content Acceleration Pack (CAP) web application in HP Executive Scorecard 9.40 an

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Executive Scorecard	9.40	All	All	All
Application	Hp	Executive Scorecard	9.41	All	All	All
Application	Hp	Executive Scorecard	9.40	All	All	All
Application	Hp	Executive Scorecard	9.41	All	All	All

References

Reference	Source	Link
Security Advisory SA59363 - HP IT Executive Scorecard Multiple Vulnerabilities - Secunia	SECUNIA	sec
Zero Day Initiative	MISC	zer
HP IT Executive Scorecard Bugs Let Remote Users Traverse the Directory and Execute Arbitrary Code - SecurityTracker	SECTrack	ww
HP Executive Scorecard Multiple Unspecified Remote Code Execution Vulnerabilities	BID	ww
SSRT101435	HP	h20
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)