



CVE-2014-2611

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

Summary

CVE	CVE-2014-2611
State	PUBLISHED
Assigner	hp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-19 10:50:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Directory traversal vulnerability in the fndwar web application in HP Executive Scorecard 9.40 and 9.41 allows remote auth

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

Problem Types: CWE-22 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

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
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
HP IT Executive Scorecard Bugs Let Remote Users Traverse the Directory and Execute Arbitrary Code - SecurityTracker				af854a3a-2127-42		
Security Advisory SA59363 - HP IT Executive Scorecard Multiple Vulnerabilities - Secunia				af854a3a-2127-42		
Zero Day Initiative				af854a3a-2127-42		
h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay				af854a3a-2127-42		
HP Executive Scorecard Multiple Unspecified Remote Code Execution Vulnerabilities				af854a3a-2127-42		
CVE Program record				CVE.ORG		
NVD vulnerability detail				NVD		
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						