CVE-2011-0276

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-0276
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-02 01:00:00 UTC
Updated	2018-10-10 20:09:00 UTC
Description	HP OpenView Performance Insight Server 5.2, 5.3, 5.31, 5.4, and 5.41 contains a "hidden account" in the com.trinagy.secu

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Openview Performance Insight	5.2	All	All	All
Application	Hp	Openview Performance Insight	5.3	All	All	All
Application	Hp	Openview Performance Insight	5.31	All	All	All
Application	Hp	Openview Performance Insight	5.4	All	All	All
Application	Hp	Openview Performance Insight	5.41	All	All	All
Application	Hp	Openview Performance Insight	5.2	All	All	All
Application	Hp	Openview Performance Insight	5.3	All	All	All
Application	Hp	Openview Performance Insight	5.31	All	All	All
Application	Hp	Openview Performance Insight	5.4	All	All	All
Application	Hp	Openview Performance Insight	5.41	All	All	All

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
70754
SecurityFocus
HP OpenView Performance Insight Server Backdoor Account Code Execution - CXSecurity.com

Zero Day Initiative
HP OpenView Performance Insight Server 'doPost()' Remote Arbitrary Code Execution Vulnerability
HPSBMA02627 SSRT090246 rev.2 - HP OpenView Performance Insight Server, Remote Execution of Arbitrary Code - c02695453 - HP Busir
HP OpenView Performance Insight Server Lets Remote Users Execute Arbitrary Code - SecurityTracker
IBM X-Force Exchange
HP OpenView Performance Insight Server Backdoor Account Code Execution
HP OpenView Performance Insight Hidden Default Account - Secunia.com
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**