CVE-2013-2347

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

Summary

CVE	CVE-2013-2347
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-04 04:51:00 UTC
Updated	2019-10-09 23:07:00 UTC
Description	The Backup Client Service (OmniInet.exe) in HP Storage Data Protector 6.2X allows remote attackers to execute arbitrary c

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.20	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All

Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All
Application	Hp	Storage Data Protector	6.21	-	All	All

References

Reference	Source	Link	Tags
Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory
HP Data Protector Backup Client Service Remote Code Execution	EXPLOIT-DB	www.exploit-db.com	Broken Link
SSRT101220	HP	h20565.www2.hp.com	Vendor Advisory
Blogger	MISC	ddilabs.blogspot.com	Permissions Required
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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