CVE-2010-3470

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

Summary

CVE	CVE-2010-3470
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-20 22:00:00 UTC
Updated	2010-09-21 04:00:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Workplace (aka WP) component in IBM FileNet P8 Application Engi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Filenet P8 Application Engine	3.5.1	All	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	001	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	002	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	003	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	004	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	005	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	006	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	007	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	008	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	009	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	010	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	011	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	012	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	013	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	014	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	015	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	016	All	All

Application	Ibm	Filenet P8 Application Engine	3.5.1	017	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	018	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	019	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	020	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	All	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	001	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	002	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	003	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	004	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	005	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	006	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	All	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	001	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	002	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	003	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	004	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	005	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	006	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	007	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	008	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	009	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	010	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	011	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	012	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	013	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	014	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	015	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	016	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	017	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	018	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	019	All	All
Application	Ibm	Filenet P8 Application Engine	3.5.1	020	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	All	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	001	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	002	All	All

Application	Ibm	Filenet P8 Application Engine	4.0.2	003	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	004	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	005	All	All
Application	Ibm	Filenet P8 Application Engine	4.0.2	006	All	All

References

Reference	Source	Link
PJ37179: Cross-site scripting vulnerabilities in Workplace are reported by Hailstorm Web Application security program.	AIXAPAR	www-0
download2.boulder.ibm.com/sar/CMA/IMA/00y3y/0/readme-4027-P8AE-FP007.htm	CONFIRM	downlo
Malformed Request	BID	www.se
download2.boulder.ibm.com/sar/CMA/IMA/00yrk/0/readme-ae351-021.htm	CONFIRM	downlo
IBM FileNet Application Engine Open Redirection and Cross Site Scripting Vulnerabilities	BID	www.se
IBM FileNet Application Engine Redirection and Cross-Site Scripting - Advisories - Community	SECUNIA	secunia
IBM FileNet Application Engine Multiple Vulnerabilities - Advisories - Community	SECUNIA	secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vu
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

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