CVE-2008-1001

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

Summary

CVE	CVE-2008-1001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-19 00:44:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Apple Safari before 3.1, when running on Windows XP or Vista, allows remote att

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	3.0	All	All	All
Application	Apple	Safari	3.0.1	All	All	All
Application	Apple	Safari	3.0.2	All	All	All
Application	Apple	Safari	3.0.3	All	All	All
Application	Apple	Safari	3.0.4	All	All	All
Application	Apple	Safari	3.0	All	All	All
Application	Apple	Safari	3.0.1	All	All	All
Application	Apple	Safari	3.0.2	All	All	All
Application	Apple	Safari	3.0.3	All	All	All
Application	Apple	Safari	3.0.4	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Xp	-	All	All	All
Operating System	Microsoft	Windows Xp	-	All	All	All

References

Reference	Source	Link

Safari Multiple Input Validation and Processing Bugs Permit Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.securitytrack
IBM X-Force Exchange	XF	exchange.xforce.il
RETIRED: Apple Safari Prior to 3.1 Multiple Security Vulnerabilities	BID	www.securityfocus
About the security content of Safari 3.1	CONFIRM	docs.info.apple.co
Apple Safari Error Page Cross-Site Scripting Vulnerability	BID	www.securityfocus
US-CERT Technical Cyber Security Alert TA08-079A -- Apple Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov
APPLE-SA-2008-03-18 Safari 3.1	APPLE	lists.apple.com
Webmail - OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**