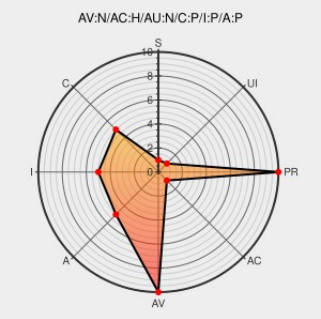
CVE-2005-1477

Published on: 05/09/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

CVE-2005-1477

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Firefox from Mozilla contain the following vulnerability:

The install function in Firefox 1.0.3 allows remote web sites on the browser's whitelist, such as update.mozilla.org or addon.mozilla.org, to execute arbitrary Javascript with chrome privileges, leading to arbitrary code execution on the system when combined with vulnerabilities such as CVE-2005-1476, as demonstrated using a javascript: URL as the package icon and a cross-site scripting (XSS) attack on a vulnerable whitelist site.

CVE-2005-1477 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Mozilla Firefox Install Method Remote Arbitrary Code Execution Vulnerability	cve.report (archive) text/html	BID 13544
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-0493
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:434
	ftp.sco.com text/plain	SCO SCOSA-2005.49
292691 – Full Remote Compromise using some of my previous vulns	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=292691

SCO OpenServer Release 5.0.7 Maintenance Pack 4 Released - Multiple Vulnerabilities Fixed	cve.report (archive) text/html	BID 15495
Firefox Full Remote Compromise	Exploit web.archive.org text/html Inactive Link Not Archived	MISC greyhatsecurity.org/vulntests/ffrc.htm
Secunia - Advisories - Mozilla Firefox Two Vulnerabilities	Patch web.archive.org text/html	SECUNIA 15292
'[Full-disclosure] Firefox Remote Compromise Leaked' - MARC	marc.info text/html	FULLDISC 20050508 Firefox Remote Compromise Leaked
US-CERT Vulnerability Note VU#648758	US Government Resource www.kb.cert.org text/html	CERT-VN VU#648758
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9231
SecurityTracker.com Archives - Firefox onload() History Access Bug and Install Function Scripting Execution Flaw Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1013913
GREYHATSECURITY.ORG	Exploit web.archive.org text/html Inactive Link Not Archived	MISC greyhatsecurity.org/firefox.htm
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100001
'[Full-disclosure] Firefox Remote Compromise Technical Details' - MARC	marc.info text/html	FULLDISC 20050508 Firefox Remote Compromise Technical Details
293302 – Firefox 1.0.3 Critical Vulnerability	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=293302
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:435
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mozilla-javascript-code-execution(20443)
MFSA 2005-42: Code execution via javascript: IconURL	www.mozilla.org text/html	CONFIRM www.mozilla.org/security/announce/mfsa2005-42.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	1.0.3	All	All	All

Application	Mozilla	Firefox	1.0.3	All	All	All

cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:mozilla:firefox:1.0.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→