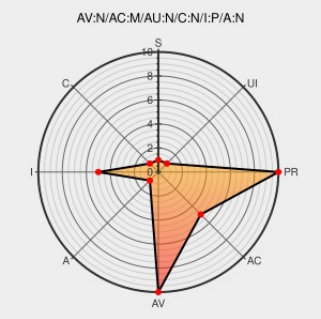
CVE-2015-6510

Published on: 08/18/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6510

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



Certain versions of Pfsense from Netgate contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in pfSense before 2.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) srctrack, (2) use_mfs_tmp_size, or (3) use_mfs_var_size parameter to system_advanced_misc.php; the (4) port, (5) snaplen, or (6) count parameter to diag_packet_capture.php; the (7) pppoe_resethour, (8) pppoe_resetminute, (9) wpa_group_rekey, or (10) wpa_gmk_rekey parameter to interfaces.php; the (11) pppoe_resethour or (12) pppoe_resetminute parameter to interfaces_ppps_edit.php; the (13) member[] parameter to interfaces_qinq_edit.php; the (14) port or (15) retry parameter to load_balancer_pool_edit.php; the (16) pkgrepourl parameter to pkg_mgr_settings.php; the (17) zone parameter to services_captiveportal.php; the port parameter to (18) services_dnsmasq.php or (19) services_unbound.php; the (20) cache_max_ttl or (21) cache_min_ttl parameter to services_unbound_advanced.php; the (22) sshport parameter to system_advanced_admin.php; the (23) id, (24) tunable, (25) descr, or (26) value parameter to system_advanced_sysctl.php; the (27) firmwareurl, (28) repositoryurl, or (29) branch parameter to system_firmware_settings.php; the (30) pfsyncpeerip, (31) synchronizetoip, (32) username, or (33) passwordfld parameter to system_hasync.php; the (34) maxmss parameter to vpn_ipsec_settings.php; the (35) ntp_server1, (36) ntp_server2, (37) wins_server1, or (38) wins_server2 parameter to vpn_openvpn_csc.php; or unspecified parameters to (39) load_balancer_relay_action.php, (40) load_balancer_relay_action_edit.php, (41) load_balancer_relay_protocol.php, or (42) load_balancer_relay_protocol_edit.php.

CVE-2015-6510 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
	Vendor Advisory www.pfsense.org text/plain	CONFIRM www.pfsense.org/security/advisories/pfSense-SA-15_06.webgui.asc

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgate	Pfsense	All	All	All	All

cpe:2.3:a:netgate:pfsense:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→