IR Number	FG-IR-17-242
Date	Nov 23, 2017
Risk	●●●○○
Impact	Cross-site Scripting (XSS), URL Redirection Attack
CVE ID	CVE-2017-14186 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14186)

PSIRT Advisory

FortiGate SSL VPN web portal login redir XSS vulnerability

Summary

A Cross-site Scripting (XSS) vulnerability in FortiOS SSL-VPN portal may allow an authenticated user to inject arbitrary web code or HTML in the context of the victim's browser via the login redir parameter.

An URL Redirection Attack may also enable an authenticated user to redirect the victim to an arbitrary URL, via the redir parameter.

Impact

Cross-site Scripting (XSS), URL Redirection Attack

Affected Products

FortiOS 5.6.0 -> 5.6.2
FortiOS 5.4.0 -> 5.4.6
FortiOS 5.2.0 -> 5.2.12
FortiOS 5.0 and below

Solutions

FortiOS 5.6 branch: Upgrade to upcoming 5.6.3 (ETA: November 27th)

FortiOS 5.4 branch: Upgrade to 5.4.6 special build (*) or upcoming 5.4.7 (ETA Dec 7th)

FortiOS 5.2 branch: Upgrade to 5.2.12 special build (*) or upcoming 5.2.13 (ETA: Dec 14th)

(*) Reach out to your local TAC to request the special build

Acknowledgement

Fortinet is pleased to thank Stefan Viehbck from SEC Consult Vulnerability Lab for reporting this vulnerability under responsible disclosure.

- (https://www.fortinet.com)