► Home (/) / PSIRT (/psirt) / FG-IR-17-113

At a glance:

IR Number	FG-IR-17-113
Date	Oct 24, 2017
Risk	● ● ● ○ ○
Impact	Cross-site scripting (XSS)
CVE ID	CVE-2017-7733 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7733)

PSIRT Advisory

FortiOS web GUI logindisclaimer redir parameter XSS vulnerability

Summary

A reflected XSS vulnerability exists in FortiOS web GUI "Login Disclaimer" redir parameter. It is potentially exploitable by a remote unauthenticated attacker, via sending a maliciously crafted URL to a victim who has an open session on the web GUI. Visiting that malicious URL may cause the execution of arbitrary javascript code in the security context of the victim's browser.

Impact

Cross-site scripting (XSS)

Affected Products

Branch 5.6: FortiOS 5.6.0

Branch 5.4: FortiOS 5.4.0 to 5.4.5

Other branches are not affected

Solutions

Branch 5.6: Upgrade to FortiOS 5.6.1 or above

Branch 5.4: Upgrade to FortiOS 5.4.6 or above.

Acknowledgement

Fortinet is pleased to thank Starhub Singapore and Andrew Ho, Maximus Consulting, and Donato Onofri of DXC Technology for reporting this vulnerability under responsible disclosure.