YOUR GLOBAL CYBER-SECURITY PARTNER

INCIDENT REPORT

Organization	Inspira health Network
Date	December 29,2017
Service	MSS-VME
Severity Level	Medium
Impact Level	Medium
Vulnerability Level	Medium

Description

Vulnerable Hosts:
https://170.75.33.4/euweb/login
https://access.ihn.org/ (170.75.33.140)
https://inspirahealthnetwork.org/

In our Monitoring System (GOC) with the MSS-VME, we detected the followings vulnerabilities.

1. This servers have SSL 2, which is OBSOLTE and INSECURE (they are vulnerable to the DROWN attack for example). It is advisable to disable it.

1.1. This servers are vulnerable to the POODLE attack. To mitigate this, SSL 3 should be disabled.

Affected Systems

Port	Host
443 / tcp / www	170.75.33.55,170.75.49.35
4443 / tcp / www	170.75.33.134, 170.75.33.139

2. The behavior of the site http://www.inspirahealthnetwork.org/ is different by https://inspirahealthnetwork.org/.

GLESEC recommends to correctly redirect the traffic.

Wrongly redirected site

Site that the URL should redirect to.

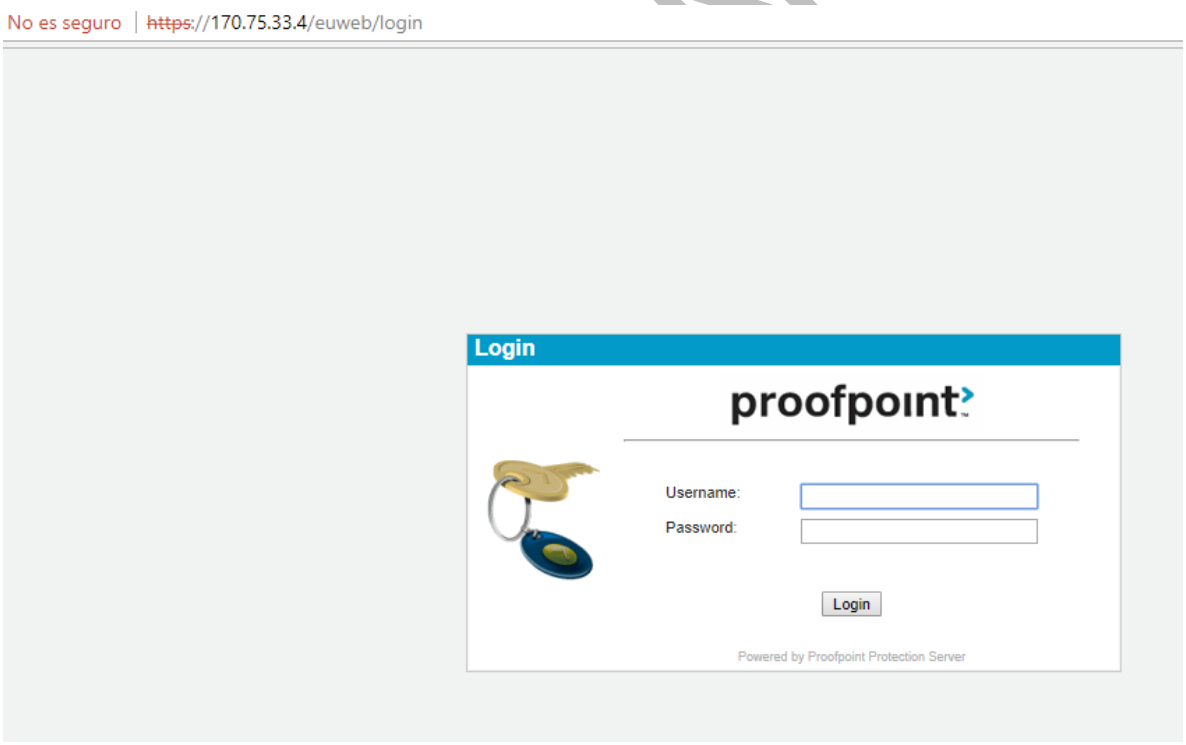
3. SSL Certificate Expired (GLESEC recommend Purchase or generate a new SSL certificate to replace the existing one)

Affected Systems

Port	Host
25 / tcp / smtp	170.75.33.4, 170.75.33.53
443 / tcp / www	170.75.33.118, 170.75.33.140

If external (Internet) access is needed for this site, please consider to improve security measures; if not, please disable this site or external access at least.

We attach the images, showing the stated above.



For any questions please do not hesitate to contact us.

Sincerely,

GLESEC OPERATIONS CENTER -GOC