GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network
Date	August 31th 2018
Service	MSS-APS
Severity Level	Medium
Impact Level	Medium
Vulnerability Level	Medium

INCIDENT DESCRIPTION

Our GOC detected that among the most frequent attack destination hosts, are a DNS server and a Microsoft Lync server. The DNS servers that are exposed to the internet must not contain records that point to the local networks, because it could leak sensitive information about the network to unauthorized third parties.

Microsoft Lync is used to organize meetings through a web portal that requires user authentication. If the web portal is not correctly configured it could be used as an entrance to attackers into the network.

Based on the information available, we must confirm if these servers should be exposed to the internet.

The exposed systems are the following:

- 170.75.32.21
- 170.75.33.109

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

GLESEC INCIDENT REPORT

TLP-AMBER

COMMENTS AND RECOMMENDATIONS

- Verify if the mentioned hosts should be exposed to the Internet.
- Limit the external access to those servers, only to the authorized parties if needed.

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY INCIDENTE REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355