GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network.
Date	09/24/2018
Service	MSS-VM
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

INCIDENT DESCRIPTION

GLESEC Operation's Center discovered 1 Critical severity vulnerability on host 170.75.48.100, it was detected a "Cisco ASA / IOS IKE Fragmentation Vulnerability". This is a well know vulnerability that is caused by missing security updates on the target CISCO device. This vulnerability may let an attacker affect your systems in these ways:

- An overflow condition exists in both the IKE and IKEv2 implementations due to improper validation of user-supplied input when handling UDP packets. An unauthenticated, remote attacker can exploit this issue, via specially crafted UDP packets, to cause a buffer overflow condition, resulting in a denial of service or the execution of arbitrary code. (CVE-2016-1287)

- A denial of service vulnerability exists in the IKEv2 implementation due to improper handling of fragmented IKEv2 packets. An unauthenticated, remote attacker can exploit this issue, via specially crafted UDP packets, to cause the device to reload. (CVE-2016-1344)

ACTIONS TO BE TAKEN

Apply the security update required to the affected host as specified on the links in the comments and recommendation section.

GLESEC INCIDENT REPORT

TLP-AMBER

COMMENTS AND RECOMMENDATIONS

GLESEC recommends mitigating this vulnerability as soon as possible. Upgrade to the relevant fixed version referenced in Cisco Security Advisories cisco-sa-20160210-asa-ike and cisco-sa-20160323-ios-ikev2.

Some relevant links from official sources are:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ios-ikev2

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