View this email in your browser

TechTopics

WITH DSI ENGINEERS
DISYS Solutions Inc.

Issue #02 February 21, 2020

This newsletter is brought to you by the DSI Engineering Team and focuses on technical topics. The goal is to share information about important updates, new partner products & solutions, and current industry news. We hope you enjoy the newsletter and feel free to send feedback anytime!

In This Issue:

Cisco Security Announcements

Firepower Management Center Vulnerability

Cisco recently published a security advisory about a vulnerability in the web management interface of Cisco Firepower Management Center (FMC). The vulnerability could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected product.

Please review this advisory for complete details as it is rated critical!

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-fmc-auth

The vulnerability affects Cisco FMC software if it is configured to authenticate users of the web-based management interface through an external LDAP server. Fixed software versions are available and listed on the advisory. To upgrade to a release that fixes this vulnerability, follow the Cisco Firepower Management Center Upgrade Guide and review the release notes of the respective release. If you are installing a hot fix patch instead, also review the upgrade guide and consult the Firepower Hot Fix Release Notes. If you have any questions, please reply to this email or contact your DSI Account Manager for assistance.

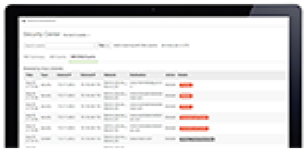
Cisco Discovery Protocol Vulnerability

The Cisco Product Security Incident Response Team (PSIRT) recently disclosed multiple vulnerabilities in the Cisco Discovery Protocol implementation of several Cisco products, along with software fix information and mitigations where available.

The CDP is a Layer 2 protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. This protocol facilitates the management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about each other. Get more details about the vulnerabilities, affected products, and associated fixes here.

Cisco Meraki Updates

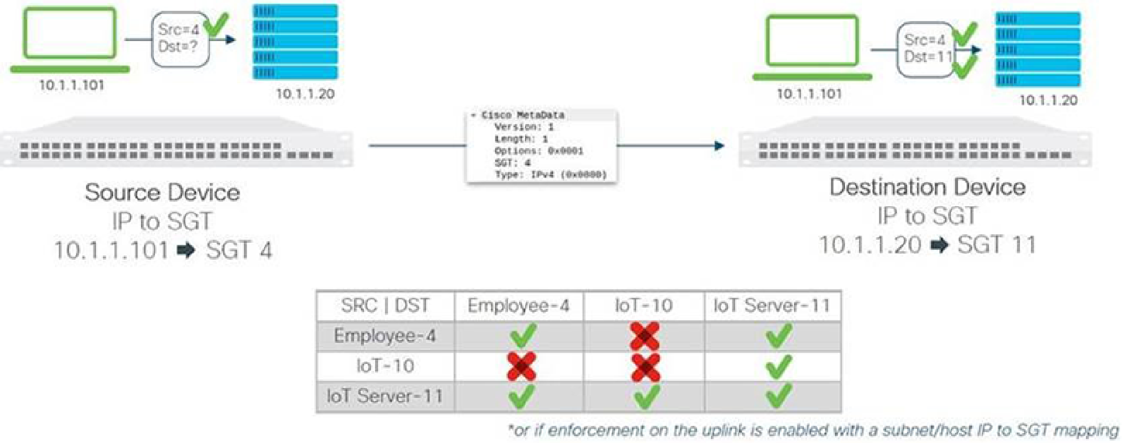
Meraki Brings Umbrella Power to Dashboard



You can bring the power of Umbrella DNS protection to the dashboard with Meraki MR advanced licenses (or upgraded licenses for your existing MR). Learn more here.

Best of Cisco’s Trustsec with Meraki MS

Adaptive Policy is a new solution where revolutionary Cisco Security Group Tag (SGT) technology meets the most powerful Cisco Meraki switch hardware yet. This software feature addresses the shortcomings of traditional policy administration using Cisco SGT and the MS390. With Cisco SGT, numerical tags are used to profile users, devices, services, and time of access. Tags can be assigned using a RADIUS server like Cisco Identity Services Engine (ISE). When Cisco ISE is used, the tag is transmitted to all devices in the network — every packet is tagged and decisions based on the tag are made by the MS390.



```
▾ Cisco MetaData
    Version: 1
    Length: 1
    Options: 0x0001
    SGT: 4
    Type: IPv4 (0x0000)
```

SRC | DST	Employee-4	IoT-10	IoT Server-11
Employee-4	✓	✗	✓
IoT-10	✗	✗	✓
IoT Server-11	✓	✓	✓

**or if enforcement on the uplink is enabled with a subnet/host IP to SGT mapping*

DSI
DISYS Solutions Inc.
DSITECH.COM

DSI provides complete IT solutions and services that are secure, innovative, energy efficient, and cost effective. Our customers include State & Local Government and Education (SLED), Federal agencies, and commercial companies. We hold nationwide contracts that are supported by a team of industry professionals and certified engineers. Learn more at dsitech.com.