# Security Advisory 05.17.2018

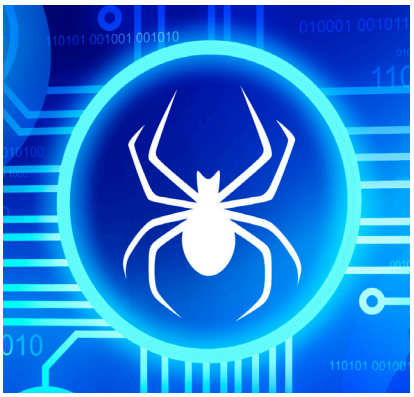
SyCom Connected.

## VULNERABILITY DETAILS & ACTION PLAN

Cisco has released updates to address vulnerabilities affecting multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

NCCIC encourages users and administrators to review the following Cisco Security Advisories and apply the necessary updates:

- Digital Network Architecture Center Static Credentials Vulnerability ▸ Click cisco-sa-20180516-dnac for link to update
- Digital Network Architecture Center Authentication Bypass Vulnerability ▸ Click cisco-sa-20180516-dna2 for link to update
- Digital Network Architecture Center Unauthorized Access Vulnerability ▸ Click cisco-sa-20180516-dna for link to update
- Enterprise NFV Infrastructure Software Linux Shell Access Vulnerability ▸ Click cisco-sa-20180516-nfvis for link to update
- Meeting Server Media Services Denial-of-Service Vulnerability ▸ Click cisco-sa-20180516-msms for link to update
- Identity Services Engine EAP TLS Certificate Denial-of-Service Vulnerability ▸ Click cisco-sa-20180516-iseeap for link to update
- IoT Field Network Director Cross-Site Request Forgery Vulnerability ▸ Click cisco-sa-20180516-fnd for link to update



### *Need help?*

*SyCom will be happy to assist with remediation efforts related to any vulnerability your business might experience. Contact your Account Manager to explore ways we can help.*

*1.888.867.9266*

*804.262.7100*