PTA Cert

Security Advisory-No: 14 **13, July 2018**

Threat Classification: Vulnerability

Name:

- Cisco Digital Network Architecture (DNA) vulnerabilities:

  (CVE-2018-0222, CVE-2018-0268, CVE-2018-0271)

Source: Affect following products of Cisco:

- Cisco Digital Network Architecture software

Distribution: The vulnerabilities can be exploited in following versions of Cisco products:

- Cisco DNA Center Software prior to Release 1.1.3

Exploited Vulnerabilities:

CVE-2018-0268: Hackers can exploit above vulnerabilities through insecure default configuration of the kubernetes container management system within DNA center, to bypass authentication and gain root privilege access on kubernetes service port to execute arbitrary commands with root privileges that could result in complete compromise of an affected system.

CVE-2018-0222: Hackers can exploit above vulnerabilities through undocumented, static user credentials for the default administrative account of affected software, an attacker could login to an affected system and execute arbitrary commands in root privileges mode.

CVE-2018-0271: Hackers can exploit above vulnerabilities by hosting the crafted URLs that designed to exploit vulnerability, on successful exploit, the attacker could gain unauthorized access to critical services under privilege mode in DNA center.

Recommendations:

1) Use following official patches information to fix aforementioned vulnerabilities:
   - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dnac
   - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna
   - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna2
2) Designate a relevant PoC for from your company for seeking assistance and reporting security issues.
3) In case of any incident, please report to this office.