

Cisco Releases Security Advisory

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

CERTT.NG encourages the following Cisco Security Advisories should be reviewed and the necessary updates be applied.

<https://tools.cisco.com/security/center/publicationListing.x>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh>

- **Cisco IOS XR Software for ASR 9000 Series Routers Denial of Service Vulnerability**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npspin-QYpwhFD>

- **Cisco IOS XR Software IP Service Level Agreements and Two-Way Active Measurement Protocol Denial of Service Vulnerability**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iplsla-ZA3SRrpP>

- **Cisco IOS XR Software Arbitrary File Read and Write Vulnerability**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-scp-inject-QwZOCy2>

- **Cisco IOS XR Software Authenticated User Privilege Escalation Vulnerabilities**

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privescal-dZYMrKf>

www.cerrt.ng

support@cerrt.ng

Telephone line; (+234)-0800998877665544.