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.

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

Cisco Security Advisories
https://tools.cisco.com/security/center/publicationListing.x
Cisco IOS XE SD-WAN Software Command Injection Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A
Cisco Web Security Appliance Proxy Service Denial of Service Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk
Cisco Intersight Virtual Appliance Command Injection Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-command-inject-CGyC8y2R
Cisco Small Business 220 Series Smart Switches Link Layer Discovery Protocol Vulnerabilities
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T
Cisco Identity Services Engine Privilege Escalation Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-UwqPrBM3
Cisco ATA 190 Series Analog Telephone Adapter Software Vulnerabilities
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3
Cisco AnyConnect Secure Mobility Client for Linux and Mac OS with VPN Posture (HostScan) Module Shared Library Hijacking Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q

www.cerrt.ng
support@cerrt.ng
Telephone line; (+234)-8178774580