Tonga National Computer Emergency Response Team

“CISCO Vulnerability Products Advisory”

Dear Constituents,

Cisco has released thirty security patch advisory to address a total of 32 security vulnerabilities in its products. Three flaws are rated as critical, as followed:

1. **CVE-2018-11776 Apache Struts remote code execution vulnerability.**
   - A vulnerability in Apache Struts could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system.
   - The vulnerability exists because the affected software insufficiently validates user-supplied input, allowing the use of results with no namespace value and the use of *url* tags with no value or action. In cases where upper actions or configurations also have no namespace or a wildcard namespace, an attacker could exploit this vulnerability by sending a request that submits malicious input to the affected application for processing. If successful, the attacker could execute arbitrary code in the security context of the affected application on the targeted system.
2. **Cisco Umbrella API Unauthorized Access Vulnerability (CVE-2018-0435)**
   - A vulnerability in the Cisco Umbrella API could allow an authenticated, remote attacker to view and modify data across their organization and other organizations.
   - The vulnerability is due to insufficient authentication configurations for the API interface of Cisco Umbrella. An attacker could exploit this vulnerability to view and potentially modify data for their organization or other organizations. A successful exploit could allow the attacker to read or modify data across multiple organizations.
3. **Cisco RV110W, RV130W, and RV215W Routers Management Interface Buffer Overflow Vulnerability (CVE-2018-0423).**
   - A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a denial of service condition or to execute arbitrary code.
   - The vulnerability is due to improper boundary restrictions on user-supplied input in the *Guest* user feature of the web-based management interface. An attacker could exploit this vulnerability by sending malicious requests to a targeted device, triggering a buffer overflow condition. A

successful exploit could allow the attacker to cause the device to stop responding, resulting in a denial of service condition, or could allow the attacker to execute arbitrary code.

- ***Vulnerable Products***

This vulnerability affects all releases of the following Cisco products:

- RV110W Wireless-N VPN Firewall
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

You can view the List of the Cisco products affected.
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180823-apache-struts

What to do?

- Ensure that all software on you device is up-to-date with the latest updates for the CISCO devices you have.

Reference

- https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.to
web: www.cert.to