# Security Advisory-No: 24

**04, Oct 2018**

**Threat Classification:** Vulnerability

**Name:**

- Buffer Overflow Vulnerability ***(CVE:2018-0423)***
- Command Injection Vulnerability ***(CVE:2018-0424)***
- Information Disclosure Vulnerability ***(CVE:2018-0425)***
- Directory Traversal Vulnerability ***(CVE:2018-0426)***

**Source:** Affect following products of Cisco:

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

**Exploited Vulnerabilities:**

***CVE:2018-0423:*** This 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 to execute arbitrary code and triggering the buffer overflow condition, that causes the device to stop responding.

***CVE:2018-0424:*** This vulnerability is due to improper validation of user-supplied input to scripts by the web-based management interface. An attacker could exploit this vulnerability by sending malicious requests to a targeted device, on the successful exploit, the attacker executes arbitrary commands with root privileges mode.

***CVE:2018-0425:*** This vulnerability is due to improper access control to files within the web-based management interface. An attacker could exploit this vulnerability by sending malicious requests to a targeted device, on the successful exploit, the attacker gain access to sensitive configuration information, including user authentication credentials.

***CVE:2018-0426:*** This vulnerability is due to improper validation of directory traversal character sequences within the web-based management interface. An attacker could exploit this vulnerability by sending malicious requests to the targeted device, on the successful exploit, the attacker gains the access to arbitrary files on that affected device, that resulting in the disclosure of sensitive information.

**Recommendations:**

a) Cisco fixed above vulnerabilities in firmware released 1.0.3.44 only for Cisco RV130W Wireless-N Multifunction VPN Router, however Cisco has not yet released any firmware for other affected devices.
   - https://software.cisco.com/download/home/285026142/type/282465789/release/1.0.3.44
   - https://software.cisco.com/download/home/283879340/type/282487380/release/1.2.1.7 (Keep visiting for updated firmware)
   - https://software.cisco.com/download/home/284436489/type/282487380/release/1.3.0.8 (Keep visiting for updated firmware)

b) Administrators may disable the ***Guest user account*** or ***remote management feature*** if not required.

c) Designate a PoC for your network users for seeking assistance and reporting security issues.

d) In case of any incident, please report to this office.