# Advisory Alert

**Alert Number:** AAA20210805 **Date:** August 5, 2021

**Document Classification Level :** Public Circulation Permitted

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **Critical** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-1609, CVE-2021-1610, CVE-2021-1602, CVE-2021-1593, CVE-2021-1572, CVE-2021-1251, CVE-2021-1308, CVE-2021-1309, CVE-2021-34707, CVE-2021-1522) |
| Description | Cisco has released updates addressing multiple vulnerabilities that exists in their products such as Execute arbitrary code, denial of service condition, Execute arbitrary Command, Remote Command Execution Vulnerability, Windows DLL Injection Vulnerability, Privilege Escalation Vulnerability, Link Layer Discovery Protocol Vulnerabilities, Sensitive Information Disclosure Vulnerability, Authentication Bypass Vulnerability. Cisco highly recommends to apply necessary security fixes to avoid issues. |
| Affected Products | Multiple Products |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-packettracer-dll-inj-Qv8Mk5Jx<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-info-disc-PjTZ5r6C<br>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmx-GkCvfd4 |

## Disclaimer

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**