



Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:089

30-June-2020

Threat Classification: Denial Of Service (DOS)

Name: CISCO IOS Software for Industrial Routers Arbitrary Code Execution Vulnerabilities

Affected Systems:

Cisco ASA or FTD Software with following features enabled:

- Cisco 809 and 829 Industrial ISRs
- CGR1000



Summary:

There are multiple vulnerabilities for CISCO 809 and 829 Industrial Integrated Services Routers (Industrial ISRs), and CSICO 1000 Series Connected Grid Routers (CGR1000) in IOS software which could allow a remote attacker or a local attacker to execute arbitrary code on the affected system or may crash the affected system.

| | |
|----------------------------|-----------------|
| Attack Severity | CRITICAL |
| Attack Vector | Network |
| Privileges required | None |

For more information, please find below official link:

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH>

Recommendations:

- For detailed information of fixed releases of Cisco ASA and FTD software for the aforementioned vulnerability, please visit following link:
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-iot-rce-xYRSeMNH#fs>
- When considering software upgrades, CISCO recommends to consult Cisco advisories available on the [Cisco Security Advisories and Alerts page](#) for determining the exposure and complete upgrade solution.
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, run software with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your Security/ Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.

