Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:115 **26-11-2020**

Name: CISCO Security Manager Path Traversal Vulnerability (CVE-2020- 27130)

Threat Classification: Gain Access

Affected Systems:

- This vulnerability affects Cisco Security Manager releases **4.21 and earlier.**

Summary:

A path traversal vulnerability, due to improper validation of directory traversal character sequences within the requests, exists in the Cisco Security Manager which could allow an unauthenticated, remote attacker to gain access to and modify sensitive information (read or write arbitrary files) on the affected device.

Attack Severity	**CRITICAL**
Attack Vector	Network
Attack Complexity	Low
Privileges required	None

For more information, please find below official link:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR

Recommendations:

- For detailed information of the CISCO Security Manager fixed releases and remediation of the aforementioned vulnerability, please visit following official link:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnggR#fs

- When considering software upgrades, it is recommended 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.

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