Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:096 **17-Aug-2020**

Threat Classification: Denial of Service (DoS)

Name: CISCO Small Business Smart and Managed Switches Denial of Service Vulnerability (CVE-2020-3363)

Affected Systems:

Affects the following products of CISCO Small Business Routers:

- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

Summary:

A vulnerability, due to insufficient validation of incoming IPv6 traffic, in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device by sending a crafted IPv6 packet.

Attack Severity	**HIGH**
Attack Vector	Network
Privileges required	None

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-3bLk6vA

Recommendations:

- For detailed information of the fixed releases of CISCO Small Business Smart and Managed Switches for the aforementioned vulnerability, please visit following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-3bLk6vA#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.