Advisory Alert

Alert Number: AAA20210219 **Date:** February 19, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	High	Information Disclosure Vulnerability

Description

Affected Product	Cisco
Severity	High
Affected Vulnerabilities	Information Disclosure Vulnerability (CVE-2019-15993)
Description	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to access sensitive device information. The vulnerability exists due to the affected software lacks proper authentication controls to information accessible from the web UI. A remote attacker can send a malicious HTTP request to the web UI of an affected device and gain access to sensitive device information, which includes configuration files.
Affected Products	Cisco 250 Series Smart Switches Cisco 350 Series Managed Switches Cisco 350X Series Stackable Managed Switches Cisco 550X Series Stackable Managed Switches Cisco Small Business 300 Series Managed Switches Cisco Small Business 500 Series Stackable Managed Switches Cisco Small Business 200 Series Smart Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200129-sml-bus-switch-disclos

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.