Advisory Alert

Alert Number : AAA20201207 **Date :** December 7, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Arbitrary code execution

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Arbitrary code execution (CVE-2020-3556)
Description	Cisco has released security patch updates addressing vulnerabilities that exists in their products. The vulnerability allows a local user to execute arbitrary code on the target system. The vulnerability exists due to a lack of authentication to the interprocess communication (IPC) channel listener. A local user can send specially crafted IPC messages to the AnyConnect client IPC listener and cause the targeted AnyConnect user to execute a script
Affected Products	AnyConnect Secure Mobility Client for Windows AnyConnect Secure Mobility Client for MacOS AnyConnect Secure Mobility Client for Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK

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.