Advisory Alert

Alert No: AAA190830 **Date: 30-Aug-19 10:25 AM**

Classification	The Alert : Public Circulation Permitted

Security Updates for 30th August 2019

Overview	High	Cisco REST API virtual service container and Cisco IOS XE	▪ Authentication Bypass Vulnerability
		Cisco IOS and IOS XE	▪ Denial of Service Vulnerability
	Medium	Google Chrome	▪ Arbitrary Code Execution

Description / Impact

Cisco REST API/ IOS XE

- Cisco has released security updates address a vulnerability for multiple product. This vulnerability could allow an attacker to take control of an affected system
- Affected Products: **Cisco 4000 Series Integrated Services Routers**
  Cisco ASR 1000 Series Aggregation Services Routers
  Cisco Cloud Services Router 1000V Series
  Cisco Integrated Services Virtual Router
- Officially Acknowledged by the Vendor: **Yes**

Cisco IOS /IOS XE

- Cisco has released security updates address a vulnerability in Network-Based Application Recognition (NBAR) which if exploited, an attacker could perform attacks such as denial of service.
- Affected Products: **Cisco IOS and IOS XE Software**
- Officially Acknowledged by the Vendor: **Yes**

Google Chrome

- Google Chrome is vulnerable to arbitrary code execution vulnerabilities which need to be patched immediately.
- Affected Products: **Google Chrome versions prior to 76.0.3809.132**
- Officially Acknowledged by the Vendor: **Yes**

Additional Information

Visit the links below and follow the instructions given by respective vendors.

Cisco REST API/ IOS XE	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass
Cisco IOS /IOS XE	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-nbar
Google Chrome	https://chromereleases.googleblog.com/2019/08/stable-channel-update-for-desktop_26.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.