Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 064   **23-January-2020**

Threat Classification: Remote code Execution (RCE) Vulnerability

Name: Citrix Application Delivery Controller, Gateway and SD-WAN WANOP Appliance Arbitrary Code Execution Vulnerability

Affected Systems: Affects the following products of Citrix:

- **Citrix ADC and Gateway version 13.0 all supported builds**
- **NetScaler ADC and Gateway version 12.1 all supported builds**
- **NetScaler ADC and Gateway version 12.0 all supported builds before 12.0.63.13**
- **NetScaler ADC and Gateway version 11.1 all supported builds before 11.1.63.15**
- **NetScaler ADC and Gateway version 10.5 all supported builds**
- **Citrix SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO all supported software release builds before 10.2.6b and 11.0.3b**

Summary:

A vulnerability has been identified in the Citrix ADC, Gateway and SDWAN WANOP products which could allow an unauthenticated remote attacker to execute arbitrary code on the vulnerable system. The scope of this vulnerability not only includes Citrix ADC and Gateway Virtual Appliances (VPX) hosted on any of the Citrix Hypervisor, ESX, Hyper-V, KVM, Azure, AWS, GCP or on a Citrix ADC Service Delivery Appliance (SDX), but also Citrix SDWAN WANOP edition packages.

Attack Severity	Critical
Attack Vector	Network
Privileges Required	None
Attack Type	Remote Code Execution

Citrix has strongly urged the affected customers to immediately apply the mitigation which applies equally to Citrix ADC, Gateway and SD-WAN WANOP deployments. For further details, please visit following link: https://support.citrix.com/article/CTX267027

Recommendations:

- For official recommended upgrade path, visit following website link to fix the aforementioned vulnerability:
    i.   https://www.citrix.com/downloads/citrix-adc/
    ii.   https://www.citrix.com/downloads/citrix-gateway/
    iii.   https://www.citrix.com/downloads/citrix-sd-wan/

- In all cases, ensure the availability of stable version by the relevant vendor, before upgrade.

- Whenever required, access the system 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.