Cyber Security Advisory No: 087 28-June-2020

Threat Classification: Code Execution

Name: Zoom Application Path Traversal Vulnerability (CVE-2020-6109)

Affected Systems: Affects the following Zoom Application version:

- Zoom Client App 4.6.10

Summary:

Zoom is a popular video conferencing solution that offers many features, including chat with users' contacts. Zoom client application has an exploitable path traversal vulnerability that processes messages including animated GIFs. An attacker may send a specially crafted message to a target user or a group to exploit this vulnerability which could result in code execution on the affected system.

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

For further details, please visit following official link:
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055

Recommendations:

- The newer versions of Zoom app patch this vulnerability. It is recommended that update your zoom app to the latest version.
- Please download the latest version of Zoom app from below mentioned official link: https://zoom.us/download
- Communicate the message to your users **(without any reference to this advisory)** for their safe usage of video conferencing applications.
- 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, 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.