Feb 12, 2016

LIVEPERSON SECURITY

Response to recent vulnerability in Cisco ASA Devices (CVE-2016-1287)

On February 10, 2016 Cisco released an advisory revealing a vulnerability in its ASA software in use by many global enterprises for establishing secure remote access connections over VPN.

This vulnerability does not target LivePerson's platform or services, but any organization in the world using Cisco ASA devices. In addition, at the time of advisory publication, the Cisco Product Security Incident Response Team was not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

LivePerson Response

- As soon as we became aware of this vulnerability, a dedicated Security Incident Response Team (SIRT) has been established to assess the potential impact on LivePerson services (if any) and prevent potential impact to services by applying a patch to vulnerable systems (if such exists).

- Our preliminary assessment has identified several devices that were vulnerable and patches has been applied. We are able to confirm that all applicable devices were patched by COB Friday, February 12, 2016.

- The affected devices are part of an infrastructure that is meant for LivePerson internal use only, by certain groups of authorized employees. Those devices are not in use by customers as part of LivePerson's services.

- According to our analysis, we have no reason to believe that an active exploit was executed against the LP infrastructure. We are closely monitoring our environment as well as developments and updates in the security industry in order to ensure highest levels of security and service delivery are maintained.

If you have any questions please contact your Account Team or LivePerson Support.