

Security Advisory-No: 15

30, July 2018

Threat Classification: Vulnerability

Name:

- Firmware Web UI Command Injection Vulnerability ([CVE:2018-0341](#))

Source: Affect following products of Cisco:

- IP Phone 6800 Series
- IP Phone 7800 Series
- IP Phone 8800 Series

Distribution: The vulnerabilities can be exploited in following versions of Cisco products:

- IP Phone 6800 Series with Multiplatform Firmware prior to Release 11.2(1)
- IP Phone 7800 Series with Multiplatform Firmware prior to Release 11.2(1)
- IP Phone 8800 Series with Multiplatform Firmware prior to Release 11.2(1)

Exploited Vulnerabilities:

Hackers can exploit above vulnerabilities by sending specially crafted shell commands to targeted user to a specific user input field using the web-based user interface that linked with handsets. That could result to inject and execute arbitrary shell commands, opening the door for attackers to eavesdrop on conversations, intercept rich media data, generating authorized phone calls.

Recommendations:

- 1) Use following official updates are available for registered users to fix aforementioned vulnerabilities:
 - <https://software.cisco.com/download/home/286311392?catid=280789323>
- 2) Designate a PoC for your network users for seeking assistance and reporting security issues.
- 3) In case of any incident, please report to this office.