Issued 1/26/17

A Vulnerability Found in Cisco WebEx Browser Extensions

A vulnerability has been discovered in the Cisco WebEx browser extension for Windows versions of Chrome, Firefox, and Internet Explorer, which could allow for arbitrary code execution. It has been confirmed by Cisco that this vulnerability does not affect Cisco WebEx browser extensions for Mac or Linux, or Cisco WebEx browser extensions for Microsoft Edge. The WebEx meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx. Successful exploitation of this vulnerability could result in the attacker gaining control of the affected system.

We recommend the following actions be taken:

- Install the update provided by Cisco immediately after appropriate testing.

- Users of Microsoft Windows systems can alternatively use Microsoft Edge to join and
participate in WebEx session.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the
effects of a successful attack.

- Remind users not to visit websites or follow links provided by unknown or untrusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or
attachments especially from un-trusted sources.

- Apply the Principle of Least Privilege to all systems and services.