CERT-MU AD-2016-09

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 14 October 2016

Severity Rating: High

Overview:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, conduct cross-site request forgery, execute arbitrary SQL queries, conduct click-jacking attack, submit arbitrary requests, impact system confidentiality, send continuous stream of SSL traffic and Consume excessive disk space resources on the target system. Cisco has issued updates and workaround(s) to address these vulnerabilities.

Description:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, conduct cross-site request forgery, execute arbitrary SQL queries, conduct click-jacking attack, submit arbitrary requests, impact system confidentiality, sending continuous stream of SSL traffic and consume excessive disk space resources on the target system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in Cisco IOS XE Software running on Cisco cBR-8 Converged Broadband Routers. The vulnerability is due to a logic processing error that exists if an affected device is configured with the Downstream Resiliency and Downstream Resiliency Bonding Group features. An attacker could exploit this vulnerability by continuously trying to establish Telnet or SSH connections to targeted device. On successful exploitation unauthenticated, remote attacker could cause a configuration integrity change to the vty line configuration on an affected device.

- A vulnerability has been identified in Cisco Finesse Agent and Supervisor Desktop Software. The vulnerability is due to insufficient CSRF protections. This vulnerability could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against the user of the web interface. An attacker could exploit this vulnerability by convincing the user of the affected system to follow a malicious link or visit an attacker-controlled website. A successful exploit could allow the attacker to submit arbitrary requests to the affected device via the web browser with the privileges of the user.

- A vulnerability has been identified in the Cisco Prime Infrastructure and Evolved Programmable Network Manager SQL database interface. The vulnerability is due to a lack of input validation on user-supplied input within SQL queries. An attacker could exploit this vulnerability by sending crafted URLs that contain malicious SQL statements to the affected system and moreover it could allow an authenticated remote attacker to impact system confidentiality by executing a subset of arbitrary SQL queries that can cause product instability. A successful exploitation of this vulnerability could allow the attacker to determine the presence of certain values in the database. Repeated exploitation could result in a sustained denial of service (DoS) condition.

- A vulnerability has been identified in Cisco Unified Communications Manager (CUCM) The vulnerability is due to a lack of proper input sanitization of *iframe* data within the HTTP requests sent to the device. An attacker could exploit this vulnerability by sending crafted HTTP packets with malicious *iframe* data. On successful exploitation a remote user can conduct click-jacking attacks or phishing attack where the user is tricked into clicking on a malicious link. Protection mechanisms should be used to prevent this type of attack.

- A vulnerability has been identified in the SSL session cache management of Cisco Wide Area Application Services (WAAS). The vulnerability is due to a lack of file size limitations for SSL system files stored on the disk. This vulnerability could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to high consumption of disk space. The user would see performance degradation. An attacker could exploit this vulnerability by sending continuous stream of SSL traffic to the targeted device. A successful exploitation will allow the attacker to cause a DoS condition due to the adverse impact on device performance.

Impact of the attack(s)

Remote attackers can:

- Cause denial of service conditions
- Conduct cross-site request forgery
- Execute arbitrary SQL queries
- Conduct click-jacking attack
- Impact system confidentiality
- Submit arbitrary requests
- Send continuous stream of SSL traffic
- Consume excessive disk space resources on the target system

Affected System:

- Releases of Cisco IOS XE Software running on Cisco cBR-8 Converged Broadband Routers:
  - All 3.16S releases, All 3.17S releases, Release 3.18.0S, Release 3.18.1S, Release 3.18.0SP
- Cisco Finesse
- Cisco Prime Infrastructure
- Cisco Evolved Programmable Network Manager
- Cisco Unified Communications Manager (CUCM)
- Cisco Wide Area Application Services (WAAS)

CVE Information:

CVE-2016-6438
CVE-2016-6442
CVE-2016-6443
CVE-2016-6440
CVE-2016-6437

Solution

Users are advised to apply updates.
More information about the updates is available on:

References:

Security Tracker

http://securitytracker.com/id/1037006

http://securitytracker.com/id/1037005
http://securitytracker.com/id/1037004
http://securitytracker.com/id/1037003
http://securitytracker.com/id/1037002

Cisco

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-cbr-8
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-fin
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-prime
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-ucm
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-waas

Cisco Security Advisories and Alerts

https://tools.cisco.com/security/center/publicationListing.x

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu