CERT-MU Advisory

CERT-MU

CERT-MU AD-2016-08

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 07 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, obtain potentially sensitive information, disclose and modify user information, obtain root privileges, obtain complete control over an affected system, conduct cross-site scripting attack on the target system, execute arbitrary code and cause the target system to reload. 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, obtain potentially sensitive information, disclose and modify user information, obtain root privileges, obtain complete control over an affected system, conduct cross-site scripting attack on the target system, execute arbitrary code and cause the target system to reload.

The vulnerabilities reported are as follows:

- A Vulnerability has been identified in Cisco NX-OS - Overlay Transport Virtualization (OTV) generic routing encapsulation (GRE) implementation of the Cisco Nexus 7000 and 7700 Series Switches. The vulnerability exists due to incomplete input validation performed on the size of OTV packet header parameters, which can result in a buffer overflow. On successful exploitation a remote user can execute arbitrary code on the target system and furthermore send specially crafted packet header parameters in a UDP packet to the Overlay Transport Virtualization (OTV) interface trigger a buffer overflow in the generic routing encapsulation (GRE) implementation and cause the target OTV process to reload or execute arbitrary code.

- A vulnerability has been identified in Cisco NX-OS - SSH subsystem of the Cisco Nexus family of products The vulnerability exists due to the improper processing of certain parameters that are passed to an affected device during the negotiation of an SSH connection. An attacker could exploit this vulnerability by authenticating to an affected device and passing a malicious value as part of the login procedure. On successful exploitation an attacker could bypass AAA restrictions and execute commands on the device command-line interface (CLI) that should be restricted to a different privileged user role.

- A vulnerability has been identified in Cisco NX-OS - DHCPv4 relay agent and smart relay agent. The Vulnerability exists due to improper validation of crafted DHCPv4 offer packets. On successful exploitation of the vulnerabilities, an attacker can send crafted DHCPv4 offer packets to an affected device and furthermore causing the DHCP process or device to crash. This vulnerability can be exploited using IPv4 packets only

- A vulnerability has been identified in Cisco NX-OS -Border Gateway Protocol (BGP).
  The vulnerability exists due to incomplete input validation of the BGP update messages. On successful exploitation of the vulnerabilities an attacker can send a crafted BGP update message to the targeted device, thus allowing the attacker to cause the switch to reload suddenly.

- A vulnerability has been identified in Cisco Unified Intelligence Center. The vulnerability exists due to insufficient input validation of a user-supplied value. The web-based management interface does not properly filter HTML code from user-supplied input before displaying the input, thus a remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. On successful exploitation of the vulnerabilities, a remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Cisco Unified Intelligence Center software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user

- A vulnerability has been identified in Cisco Unified Intelligence Center. The vulnerability exists due to improper implementation of authorization controls when accessing certain web pages of the application. On successful exploitation

of the vulnerabilities an attacker can access certain web pages and creating unauthorized user accounts.

- A vulnerability has been identified in Cisco Unified Intelligence Center. A remote user can conduct cross-site request forgery attacks. The vulnerability exists due to insufficient CSRF protections. 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. On successful exploitation an attacker could allow submit arbitrary requests to the affected device via the web browser with the privileges of the user.

- A vulnerability has been identified in Cisco IOS on 7600 series routers and Catalyst 6500 series switches. A remote user can bypass access controls on the target system. The vulnerability is due to the improper implementation of PACL logic for ACEs that include a greater than operator, a less than operator, a *tcp* flag, the *established* keyword, or the *range* keyword. On successful exploitation an attacker could bypass the filters defined in the PACL for a targeted system.

- A vulnerability has been identified in Cisco IOS and IOS XE. A remote user can cause the target system to reload. The vulnerability exists due to improper handling of crafted IKEv2 packets. The vulnerability applies only to IKEv2 devices acting as clients or IKEv2 initiators. An attacker could exploit this vulnerability by sending crafted packets to the affected devices, however, an attacker would need to be able to force the affected device to connect to a rogue IKEv2 server under its control. A successful exploitation could allow the attacker to cause a reload of the affected system

- A vulnerability has been identified in Cisco IOS XR. A local user can obtain root privileges on the target system. The vulnerability exists due to incorrect permissions given to a set of users. An attacker could exploit this vulnerability by authenticating to the device and sending crafted user input to execute commands on the underlying operating system. The user has to be logged-in to the device with valid admin credentials.

Impact of the attack(s)

Remote attackers can:

- cause denial of service conditions
- conduct cross-site scripting attack
- gain full control of the target system
- Disclose user information
- Modify user information
- Execute arbitrary code
- obtain root privileges of the target system
- cause target system to reload

Affected System:

- Nexus 7000, 7700
- Multilayer Director Switches, Nexus 1000V Series Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 3500 Platform Switches, Nexus 4000 Series Switches, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in NX-OS mode, Nexus 9000 Series Switches in Application Centric Infrastructure (ACI) mode
- Cisco Unified Contact Center Express and Cisco Unified Intelligence Center
- Cisco Catalyst 6500 Series Switches and Cisco 7600
- Cisco IOS XR

CVE Information:

CVE-2016-1453
CVE-2015-0721
CVE-2015-6392
CVE-2015-6393
CVE-2016-1454
CVE-2016-6425
CVE-2016-6426
CVE-2016-6427
CVE-2016-6422
CVE-2016-6423
CVE-2016-6428

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

References:

Security Tracker
http://securitytracker.com/id/1036946
http://securitytracker.com/id/1036947
http://securitytracker.com/id/1036948
http://securitytracker.com/id/1036949
http://securitytracker.com/id/1036950
http://securitytracker.com/id/1036951
http://securitytracker.com/id/1036952
http://securitytracker.com/id/1036953
http://securitytracker.com/id/1036954
http://securitytracker.com/id/1036955
http://securitytracker.com/id/1036956

Cisco
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-otv
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-nxaaa
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp1
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-dhcp2
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-bgp
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis1
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis2
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ucis3
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-catalyst
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-ios-ikev
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-iosxr

Cisco Security Advisories and Alerts
https://tools.cisco.com/security/center/publicationListing.x?product=Cisco#~Vulnerabilities

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