CERT-EU Security Advisory 2018-011

Cisco Products Multiple Vulnerabilities

April 19, 2018 — v1.0

History:

- *19/04/2018 — v1.0 – Initial publication*

Summary

On the 17th and 18th of April 2018, Cisco has released several updates to address vulnerabilities [1] affecting multiple products in which a remote attacker can exploit these vulnerabilities to trigger cross site scripting, denial of service, remote code execution, security restriction bypass and sensitive information disclosure on the targeted system.

Technical Details

Vulnerabilities impact [1, 2] is presented below.

Critical

- Cisco WebEx Clients Remote Code Execution Vulnerability. CVE-2018-0112
- Cisco UCS Director Virtual Machine Information Disclosure Vulnerability for End User Portal. CVE-2018-0238
- Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability. CVE-2018-0171

High

- Cisco IOS and IOS XE Software Smart Install Denial of Service Vulnerability. CVE-2018-0156
- Cisco StarOS Interface Forwarding Denial of Service Vulnerability. CVE-2018-0239
- Cisco IOS XR Software UDP Broadcast Forwarding Denial of Service Vulnerability. CVE-2018-0241
- Cisco Firepower Detection Engine Secure Sockets Layer Denial of Service Vulnerability. CVE-2018-0233
- Cisco Firepower 2100 Series Security Appliances IP Fragmentation Denial of Service Vulnerability. CVE-2018-0230
- Cisco ASA Software, FTD Software, and AnyConnect Secure Mobility Client SAML Authentication Session Fixation Vulnerability. CVE-2018-0229
- Cisco Adaptive Security Appliance Application Layer Protocol Inspection Denial of Service Vulnerabilities. CVE-2018-0240

- Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability. CVE-2018-0231
- Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability. CVE-2018-0228
- Cisco Adaptive Security Appliance Virtual Private Network SSL Client Certificate Bypass Vulnerability. CVE-2018-0227

Medium

- Cisco WebEx Connect IM Cross-Site Scripting Vulnerability. CVE-2018-0276
- Cisco Unified Communications Manager LDAP Information Disclosure Vulnerability. CVE-2018-0267
- Cisco Unified Communications Manager HTTP Interface Information Disclosure Vulnerability. CVE-2018-0266
- Cisco StarOS IPsec Manager Denial of Service Vulnerability. CVE-2018-0273
- Cisco Packet Data Network Gateway Peer-to-Peer Message Processing Denial of Service Vulnerability. CVE-2018-0256
- Cisco Identity Services Engine Shell Access Vulnerability. CVE-2018-0275
- Cisco Industrial Ethernet Switches Device Manager Cross-Site Request Forgery Vulnerability. CVE-2018-0255
- Cisco Firepower System Software Intelligent Application Bypass Vulnerability. CVE-2018-0254
- Cisco Firepower System Software Server Message Block File Policy Bypass Vulnerability. CVE-2018-0243
- Cisco Firepower System Software Server Message Block File Policy Bypass Vulnerability. CVE-2018-0244
- Cisco Firepower Threat Defense SSL Engine High CPU Denial of Service Vulnerability. CVE-2018-0272
- Cisco DNA Center Cross Origin Resource Sharing Vulnerability. CVE-2018-0269
- Cisco cBR Series Converged Broadband Routers High CPU Usage Denial of Service Vulnerability. CVE-2018-0257
- Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability. CVE-2018-0251
- Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability. CVE-2018-0242
- Cisco AMP for Endpoints macOS Connector DMG File Malware Bypass Vulnerability. CVE-2018-0237
- Cisco MATE Live Directory Information Disclosure Vulnerability. CVE-2018-0260
- Cisco MATE Collector Cross-Site Request Forgery Vulnerability. CVE-2018-0259

Products Affected

Due to the fact that multiple products are affected, below you will find only products families. For details please consult Cisco Security Advisories and Alerts web site [1].

- Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE Software and have the Smart Install client feature enabled.
- Cisco Adaptive Security Appliance
- Cisco AMP for Endpoints
- Cisco ASA Software, FTD Software, and AnyConnect Secure Mobility Client
- Cisco cBR Series Converged Broadband Routers

- Cisco DNA Center
- Cisco Firepower System Software
- Cisco Firepower Threat Defense SSL Engine
- Cisco Identity Services Engine
- Cisco Industrial Ethernet Switches Device Manager
- Cisco IOS XR Software
- Cisco MATE Collector
- Cisco MATE Live Directory
- Cisco Packet Data Network Gateway
- Cisco StarOS
- Cisco UCS Director Virtual Machine
- Cisco Unified Communications Manager
- Cisco WebEx Clients
- Cisco WebEx Connect IM

Recommendations

Upgrade products based on Cisco recommendations [1].

Workarounds

Due to the large number of products affected please consult the specific vulnerable product workaround if any [1].

References

[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://www.us-cert.gov/ncas/current-activity/2018/04/18/Cisco-Releases-Security-Updates-Multiple-Products

[3] https://www.hkcert.org/mobile_url/en/alert/18041902