

Cisco Multiple Vulnerabilities Security Updates

Cisco has issued updates to address vulnerabilities affecting multiple products that could be exploited by remote attacker thereby enabling the attacker to gain full access to an affected system.

CERT.NG encourages the following Cisco Security Advisories should be reviewed and the necessary updates should be applied:

- Cisco IOS XE Software Static Credential Vulnerability [cisco-sa-20180328-xesc\(link is external\)](#)
- Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability [cisco-sa-20180328-smi2\(link is external\)](#)
- Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability [cisco-sa-20180328-qos\(link is external\)](#)
- Cisco IOS XE Software Web UI Remote Access Privilege Escalation Vulnerability [cisco-sa-20180328-xepriv\(link is external\)](#)
- Cisco IOS XE Software Simple Network Management Protocol Double-Free Denial of Service Vulnerability [cisco-sa-20180328-snmp-dos\(link is external\)](#)
- Cisco IOS Software Simple Network Management Protocol GET MIB Object ID Denial of Service Vulnerability [cisco-sa-20180328-snmp\(link is external\)](#)
- Cisco IOS and IOS XE Software Smart Install Denial of Service Vulnerability [cisco-sa-20180328-smi\(link is external\)](#)
- Cisco IOS XE Software User EXEC Mode Root Shell Access Vulnerabilities [cisco-sa-20180328-privesc1\(link is external\)](#)
- Cisco IOS XE Software with Cisco Umbrella Integration Denial of Service Vulnerability [cisco-sa-20180328-opendns-dos\(link is external\)](#)
- Cisco IOS, IOS XE, and IOS XR Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities [cisco-sa-20180328-lldp\(link is external\)](#)
- Cisco IOS XE Software for Cisco Catalyst Switches IPv4 Denial of Service Vulnerability [cisco-sa-20180328-ipv4\(link is external\)](#)
- Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability [cisco-sa-20180328-ike-dos\(link is external\)](#)
- Cisco IOS and IOS XE Software Internet Key Exchange Memory Leak Vulnerability [cisco-sa-20180328-ike\(link is external\)](#)

- Cisco IOS XE Software Internet Group Management Protocol Memory Leak Vulnerability [cisco-sa-20180328-igmp\(link is external\)](#)
- Cisco IOS XE Software Zone-Based Firewall IP Fragmentation Denial of Service Vulnerability [cisco-sa-20180328-fwip\(link is external\)](#)
- Cisco IOS Software Integrated Services Module for VPN Denial of Service Vulnerability [cisco-sa-20180328-dos\(link is external\)](#)
- Cisco IOS and IOS XE Software DHCP Version 4 Relay Denial of Service Vulnerability [cisco-sa-20180328-dhcpr3\(link is external\)](#)
- Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability [cisco-sa-20180328-dhcpr2\(link is external\)](#)
- Cisco IOS and IOS XE Software DHCP Version 4 Relay Heap Overflow Denial of Service Vulnerability [cisco-sa-20180328-dhcpr1\(link is external\)](#)
- Cisco IOS and IOS XE Software Bidirectional Forwarding Detection Denial of Service Vulnerability [cisco-sa-20180328-bfd](#)

Reference:

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2>