

CVE-2020-3161

Cisco IP Phones Web Server Remote Code Execution and Denial-of-Service Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A vulnerability in the web server for Cisco IP Phones could allow an unauthenticated, remote attacker to execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web server of a targeted device. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a DoS condition.

EVRS

83/100

Urgent priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.839

99.69th percentile · FIRST

CISA DEADLINE

May 3, 2022

KEV since 2021 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.839 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 18 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ip phone 8865 firmware	10.3\ (1\)es14 11.0\ (1\) 11.0\ (5\)sr1	no fixed version listed	NVD
ip phone 8851 firmware	10.3\ (1\)es14 11.0\ (1\) 11.0\ (5\)sr1	no fixed version listed	NVD
ip phone 7841 firmware	11.0\ (1\)	no fixed version listed	NVD
ip phone 7821 firmware	11.0\ (1\)	no fixed version listed	NVD
ip phone 8811 firmware	10.3\ (1\)es14 11.0\ (1\) 11.0\ (5\)sr1	no fixed version listed	NVD
ip phone 8861 firmware	10.3\ (1\)es14 11.0\ (1\) 11.0\ (5\)sr1	no fixed version listed	NVD
ip phone 8845 firmware	10.3\ (1\)es14 11.0\ (1\) 11.0\ (5\)sr1	no fixed version listed	NVD
ip phone 7861 firmware	11.0\ (1\)	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-74vv-6p4c-8fhj

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phones-rce-dos-rB6EeRXs

NVD nvd.nist.gov/vuln/detail/CVE-2020-3161

CISA KEY cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-24432

Current data evulnable.com/vulnerability-management/cve/CVE-2020-3161

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.