# CVE Detail – CVE-2020-3161

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.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.99084

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-20: Improper Input Validation

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-101: Server Side Include (SSI) Injection
* CAPEC-104: Cross Zone Scripting
* CAPEC-108: Command Line Execution through SQL Injection
* CAPEC-109: Object Relational Mapping Injection
* CAPEC-110: SQL Injection through SOAP Parameter Tampering
* CAPEC-120: Double Encoding
* CAPEC-13: Subverting Environment Variable Values
* CAPEC-135: Format String Injection
* CAPEC-136: LDAP Injection
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-153: Input Data Manipulation
* CAPEC-182: Flash Injection
* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-22: Exploiting Trust in Client
* CAPEC-23: File Content Injection
* CAPEC-230: Serialized Data with Nested Payloads
* CAPEC-231: Oversized Serialized Data Payloads
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-250: XML Injection
* CAPEC-261: Fuzzing for garnering other adjacent user/sensitive data
* CAPEC-267: Leverage Alternate Encoding
* CAPEC-28: Fuzzing
* CAPEC-3: Using Leading 'Ghost' Character Sequences to Bypass Input Filters
* CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies
* CAPEC-42: MIME Conversion
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-473: Signature Spoof
* CAPEC-52: Embedding NULL Bytes
* CAPEC-53: Postfix, Null Terminate, and Backslash
* CAPEC-588: DOM-Based XSS
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-664: Server Side Request Forgery
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-7: Blind SQL Injection
* CAPEC-71: Using Unicode Encoding to Bypass Validation Logic
* CAPEC-72: URL Encoding
* CAPEC-73: User-Controlled Filename
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic
* CAPEC-81: Web Server Logs Tampering
* CAPEC-83: XPath Injection
* CAPEC-85: AJAX Footprinting
* CAPEC-88: OS Command Injection
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities

## ATT&CK Techniques

* T1574.007: Path Interception by PATH Environment Variable
* T1539: Steal Web Session Cookie
* T1553.002: Code Signing
* T1574.006: Dynamic Linker Hijacking
* T1562.003: Impair Command History Logging
* T1027: Obfuscated Files or Information
* T1036.001: Invalid Code Signature

## Used By (Actors/Tools)

* TrickBot (malware)
* EKANS (malware)
* BLINDINGCAN (malware)
* SynAck (malware)
* Bumblebee (malware)
* Amadey (malware)
* Orz (malware)
* NOKKI (malware)
* Stuxnet (malware)
* AvosLocker (malware)
* COATHANGER (malware)
* Sardonic (malware)
* WindTail (malware)
* Matryoshka (malware)
* StrongPity (malware)
* Janicab (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* NETWIRE (malware)
* OLDBAIT (malware)
* GreyEnergy (malware)
* TEARDROP (malware)
* Turian (malware)
* Action RAT (malware)
* Gootloader (malware)
* PolyglotDuke (malware)
* Hildegard (malware)
* SombRAT (malware)
* Snip3 (malware)
* RegDuke (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* TRANSLATEXT (malware)
* Regin (malware)
* Line Dancer (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Diavol (malware)
* Siloscape (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* DRATzarus (malware)
* BOOSTWRITE (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Conficker (malware)
* Flagpro (malware)
* SpicyOmelette (malware)
* Green Lambert (malware)
* LockerGoga (malware)
* ISMInjector (malware)
* PUNCHBUGGY (malware)
* POSHSPY (malware)
* MiniDuke (malware)
* Anchor (malware)
* DarkTortilla (malware)
* ROKRAT (malware)
* CORESHELL (malware)
* PlugX (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Epic (malware)
* Cuba (malware)
* Clambling (malware)
* DarkGate (malware)
* SVCReady (malware)
* Carbanak (malware)
* XTunnel (malware)
* Hydraq (malware)
* Gazer (malware)
* Saint Bot (malware)
* Chaes (malware)
* Bundlore (malware)
* EVILNUM (malware)
* Metamorfo (malware)
* Spica (malware)
* Trojan.Karagany (malware)
* Bandook (malware)
* PipeMon (malware)
* Shamoon (malware)
* BLUELIGHT (malware)
* BPFDoor (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* OopsIE (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* SDBbot (malware)
* RTM (malware)
* SodaMaster (malware)
* StrelaStealer (malware)
* Grandoreiro (malware)
* GoBear (malware)
* Drovorub (malware)
* Bazar (malware)
* Kobalos (malware)
* XLoader (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* Final1stspy (malware)
* MgBot (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Valak (malware)
* Samurai (malware)
* PoisonIvy (malware)
* NanoCore (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* Daserf (malware)
* Carbon (malware)
* Pisloader (malware)
* Ramsay (malware)
* Pillowmint (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* Nerex (malware)
* BoomBox (malware)
* PUNCHTRACK (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* Clop (malware)
* Lokibot (malware)
* PoetRAT (malware)
* CoinTicker (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Maze (malware)
* ComRAT (malware)
* ChChes (malware)
* PowerStallion (malware)
* JPIN (malware)
* HTTPBrowser (malware)
* XCSSET (malware)
* KillDisk (malware)
* AppleJeus (malware)
* SoreFang (malware)
* Industroyer (malware)
* Agent Tesla (malware)
* ECCENTRICBANDWAGON (malware)
* BADNEWS (malware)
* ShadowPad (malware)
* QakBot (malware)
* CookieMiner (malware)
* Hancitor (malware)
* Gelsemium (malware)
* jRAT (malware)
* Helminth (malware)
* Dridex (malware)
* Denis (malware)
* Comnie (malware)
* H1N1 (malware)
* SLOWPULSE (malware)
* ADVSTORESHELL (malware)
* HiddenWasp (malware)
* Small Sieve (malware)
* HermeticWizard (malware)
* ShimRatReporter (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Empire (tool)
* PcShare (tool)
* CSPY Downloader (tool)
* CARROTBALL (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Out1 (tool)
* Imminent Monitor (tool)
* MCMD (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* OilRig (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* APT42 (intrusion-set)
* Earth Lusca (intrusion-set)
* Sandworm Team (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Operation Honeybee (campaign)
* 2016 Ukraine Electric Power Attack (campaign)
* APT38 (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* Mustang Panda (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* menuPass (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Rocke (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Windshift (intrusion-set)
* Gamaredon Group (intrusion-set)
* Sea Turtle (intrusion-set)
* Moonstone Sleet (intrusion-set)
* APT3 (intrusion-set)
* C0017 (campaign)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* APT-C-36 (intrusion-set)
* Gallmaker (intrusion-set)
* CopyKittens (intrusion-set)
* Star Blizzard (intrusion-set)
* PROMETHIUM (intrusion-set)
* BlackOasis (intrusion-set)

## Affected Products

* cpe:2.3:o:cisco:ip\_phone\_8865\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8865\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8865\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8851\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8851\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8851\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_7841\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_7821\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8811\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8811\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8811\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8861\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8861\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8861\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8845\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8845\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8845\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_7861\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8841\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8841\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8841\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_7811\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821-ex\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821-ex\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:ip\_phone\_8821-ex\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:8831\_firmware:10.3\(1\)es14:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:8831\_firmware:11.0\(1\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:cisco:8831\_firmware:11.0\(5\)sr1:\*:\*:\*:\*:\*:\*:\*