بسمه تعالی

# چندین آسیب‌پذیری بحرانی در محصولات سیسکو

## آسیب‌پذیری اجرای کد از راه دور و حمله DoS در وب سرور IP Phones سیسکو

یک آسیب‌پذیری در وب سرور IP Phones سیسکو با شناسه "CVE-2020-3161" و شدت Critical کشف شده است که می‌تواند به یک مهاجم غیرمجاز و تایید هویت نشده اجازه دهد تا کد دلخواه خود را با دسترسی root اجرا کرده و باعث reload شدن یک IP phone آسیب‌دیده و در نتیجه حمله denial of service (DoS) گردد.

این آسیب‌پذیری به دلیل عدم اعتبارسنجی مناسب در درخواست‌های HTTP است. مهاجم می‌تواند با ارسال یک درخواست ساختگی HTTP به وب سرور دستگاه مورد هدف، از این آسیب‌پذیری سوء استفاده کند.

این آسیب‌پذیری محصولات نام‌برده در زیر را در صورتیکه دسترسی به وب در آنها فعال شده باشد و یک firmware نسخه قبل تر از اولین نسخه وصله شده برای این دستگاه را داشته باشند، تحت تاثیر قرار می‌دهد:

- IP Phone 7811, 7821, 7841, and 7861 Desktop Phones
- IP Phone 8811, 8841, 8845, 8851, 8861, and 8865 Desktop Phones
- Unified IP Conference Phone 8831
- Wireless IP Phone 8821 and 8821-EX

نکته: دسترسی به وب به طور پیش‌فرض در IP phones سیسکو غیرفعال است. کاربران می‌توانند با بررسی تنظیمات Unified Communications Manager سیسکو در قسمت Device > Phone > Select a Phone و بررسی Enabled یا Disabled بودن دسترسی وب، از آسیب‌پذیر بودن دستگاه خود اطمینان حاصل کنند. در صورت Disabled بودن، IP phone آسیب‌پذیر نخواهد بود.

به کاربران توصیه می‌شود جهت ارتقاء نسخه firmware ، مطابق با جدول زیر اقدام کنند:

| Cisco IP Phone Model | Cisco Bug ID | First Fixed Release |
|---|---|---|
| IP Phone 7811, 7821, 7841, 7861 Desktop Phones | CSCuz03016 | 11.7(1) |
| IP Phone 8811, 8841, 8845, 8851, 8861, 8865 Desktop Phones | CSCuz03016 | 11.7(1) |
| Unified IP Conference Phone 8831 | CSCvs78441 | 10.3(1)SR6 |
| Wireless IP Phone 8821, 8821-EX | CSCvs78272 | 11.0(5)SR3 |

برای دانلود IP Phone firmware سیسکو در سایت Cisco.com، مراحل زیر را دنبال کنید:

۱) روی Browse all کلیک کنید.
۲) Collaboration Endpoints > IP Phones را انتخاب کنید.
۳) از بخش مربوط به product selector، یک محصول خاص را انتخاب کنید.
۴) و سپس نسخه موردنظر خود را انتخاب کنید.

## آسیب‌پذیری‌های چندگانه در UCS Director و UCS Director Express سیسکو

آسیب‌پذیری‌های چندگانه در REST API مربوط به UCS Director و UCS Director Express سیسکو برای Big Data (داده‌های بزرگ)، به یک مهاجم از راه دور اجازه می‌دهد تا فرآیند احراز هویت را دور بزند یا حملات directory traversal را بر روی یک دستگاه آسیب‌دیده اجرا کند.

محصولاتی که تحت تاثیر یک یا چند از این آسیب‌پذیری‌ها قرار می‌گیرند به شرح جدول زیر است:

| Product | Cisco Bug IDs | Vulnerable Release(s) | Fixed Release |
|---|---|---|---|
| Cisco UCS Director | CSCvs53496, CSCvs53493 CSCvs53500, CSCvs53502 CSCvs56400, CSCvs56401 CSCvs56399, CSCvs69171 CSCvs69022 | 6.0.0.0, 6.0.0.1, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.0.1.3<br>6.5.0.0, 6.5.0.1, 6.5.0.2, 6.5.0.3, 6.5.0.4<br>6.6.0.0, 6.6.1.0, 6.6.2.0<br>6.7.0.0, 6.7.1.0, 6.7.2.0, 6.7.3.0 | 6.7.4.0 |
| Cisco UCS Director Express for Big Data | CSCvt39561, CSCvt39555 CSCvt39580, CSCvt39565 CSCvt39535, CSCvt39526 CSCvt39575, CSCvt39489 | 3.7.3.0 and earlier | 3.7.4.0 |

یک آسیب‌پذیری با شناسه " CVE-2020-3240 " که به دلیل اعتبارسنجی نامناسب ورودی اتفاق می‌افتد، به مهاجم احراز هویت شده از راه دور اجازه می‌دهد تا کد دلخواه خود را با دسترسی root در سیستم‌عامل اصلی اجرا کند.

آسیب‌پذیری بعدی با شناسه " CVE-2020-3250 " ناشی از اعتبارسنجی ناکافی کنترل دسترسی است و یک مهاجم با بهره‌برداری از آن می‌تواند فرآیند احراز هویت را دور زده و API calls را بر روی دستگاه آسیب‌دیده اجراکند. یک اکسپلویت موفق، مهاجم را قادر می‌سازد تا با REST API تعامل داشته باشد و باعث یک حمله بالقوه Denial of Service (DoS) شود.

یکی دیگر از این آسیب‌پذیری‌ها که با شناسه " CVE-2020-3251 " شناخته می‌شود، به دلیل اعتبارسنجی نادرست ورودی‌های کاربر در REST API است که با اکسپلویت آن، مهاجم می‌تواند حمله directory traversal و کد دلخواه خود را بر روی سیستم اجرا کند.

آسیب‌پذیرهای دیگری با شناسه‌های CVE-2020-3249، CVE-2020-3248، CVE-2020-3247، CVE-2020-3239، CVE-2020-3252 نیز حملات directory traversal را به دنبال دارند.

شرکت سیسکو با انتشار UCS Director نسخه ۶.۷.۴.۰ و UCS Director Express نسخه ۳.۷.۴.۰، این آسیب‌پذیری‌ها را وصله کرده است.

## آسیب‌پذیری سرریز بافر در وب اپلیکیشن IP Phones سیسکو

یک آسیب‌پذیری با شناسه "CVE-2016-1421 " و شدت Critical در وب اپلیکیشن IP Phones گزارش شده است که به واسطه آن، مهاجم می‌تواند کد دلخواه خود را با دسترسی root اجرا کرده و منجر به reload شدن IP phone و در نتیجه اجرای یک حمله DoS گردد.

دلیل این آسیب‌پذیری این است که نرم‌افزار آسیب‌دیده نمی‌تواند حدود داده ورودی را بررسی کند و مهاجم با ارسال یک درخواست HTTP ساختگی به وب سرور دستگاه آسیب‌پذیر، آن را اکسپلویت می‌کند و در صورت موفقیت، قادر خواهد بود که با امتیازات root، موجب حمله DoS در دستگاه شود.

محصولات زیر، در صورت فعال بودن دسترسی وب در آنها، تحت تاثیر این آسیب‌پذیری قرار می‌گیرند:

- IP Phone 7811, 7821, 7841, and 7861 Desktop Phones
- IP Phone 8811, 8841, 8845, 8851, 8861, and 8865 Desktop Phones
- Wireless IP Phone 8821 and 8821-EX

به کاربران توصیه می‌شود مطابق جدول زیر به ارتقاء نسخه محصول مورد نظر اقدام کنند:

| Cisco IP Phone Model | Cisco Bug ID | First Fixed Release |
|---|---|---|
| IP Phone 7811, 7821, 7841, 7861 Desktop Phones | CSCuz03034 | 11.7(1) |
| IP Phone 8811, 8841, 8845, 8851, 8861, 8865 Desktop Phones | CSCuz03034 | 11.7(1) |
| Wireless IP Phone 8821, 8821-EX | CSCvs78281 | 11.0(5)SR3 |

منبع

https://tools.cisco.com/security/center/publicationListing.x