بسمه تعالی


مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

# آسیب‌پذیری در قابلیت SUBSCRIBE پروتکل UPnP

## گزارش آسیب‌پذیری

# فهرست مطالب


**۱ آسیب‌پذیری ..... ۱**

**۲ وضعیت ایران ..... ۱**

**۳ میزان تاثیرگذاری ..... ۲**

۳-۱ چه کسانی در معرض این آسیب‌پذیری قرار دارند ..... ۲

۳-۲ کاربران خانگی ..... ۲

۳-۳ ISP ..... ۳

۳-۴ فروشندگان دستگاه ..... ۳

۳-۵ شرکت ..... ۳

۳-۶ دستگاه‌های آسیب‌پذیر ..... ۳

**۴ راه‌حلها ..... ۴**

۴-۱ اعمال بروزرسانی ..... ۴

4-2 غیرفعال یا محدود کردن UPnP ..... ۵

4-3 IDS Signature ..... ۵

**۵ جمع بندی ..... ۵**

**۶ منابع: ..... ۵**

## مقدمه

بر اساس گزارشات منتشر شده، پروتکل Universal Plug and Play (UPnP) می‌تواند برای ارسال ترافیک به مقصدهای دلخواه با استفاده از قابلیت SUBSCRIBE مورد سوء استفاده قرار گیرد. این پروتکل به منظور ارائه کشف خودکار و تعامل با دستگاه‌های موجود در شبکه طراحی شده است. پروتکل UPnP به گونه‌ای طراحی شده است که در یک شبکه محلی (LAN) قابل اعتماد مورد استفاده قرار می‌گیرد و هیچ گونه احراز و تصدیق هویت را اجرا نمی‌کند.

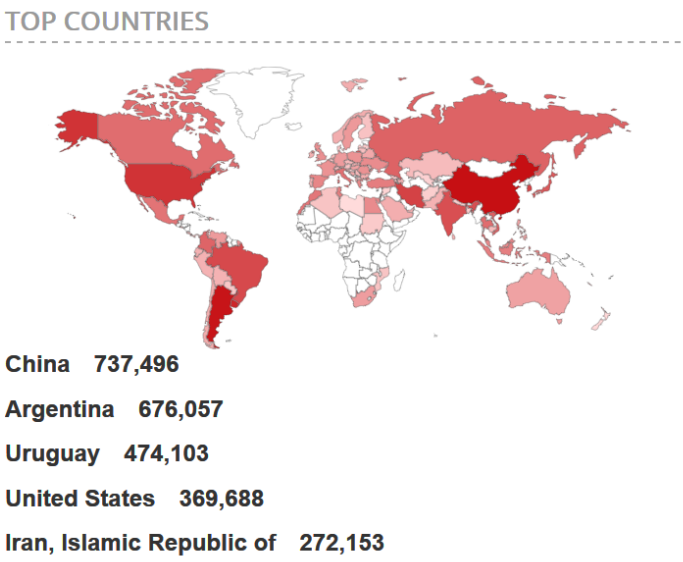
## ۱ آسیب‌پذیری

بسیاری از دستگاه‌های متصل به اینترنت، از پروتکل UPnP پشتیبانی می‌کنند. آسیب‌پذیری کشف شده در قابلیت UPnP SUBSCRIBE به مهاجمان اجازه می‌دهد تا مقادیر زیادی از داده‌ها را به مقصدهای دلخواه قابل دسترسی از طریق اینترنت ارسال کنند که این امر می‌تواند منجر به حمله Distributed Denial of Service (DDoS)، نشت و سرقت داده‌ها و سایر اعمال غیرمنتظره در شبکه شود. این آسیب‌پذیری با شناسه "CVE-2020-12695" و با عنوان Call Stranger شناخته می‌شود.

آسیب‌پذیری مذکور ناشی از مقدار Callback header در قابلیت UPnP SUBSCRIBE است که توسط یک مهاجم قابل کنترل می‌باشد و یک آسیب‌پذیری شبیه به SSRF را فعال می‌کند.

## ۲ وضعیت ایران

اگرچه ارائه خدمات UPnP در اینترنت عموماً به عنوان یک پیکربندی اشتباه تلقی می‌شود، اما بر اساس اسکن اخیر موتور جستجوی Shodan، هنوز تعداد زیادی از دستگاه‌ها از طریق اینترنت در دسترس هستند. اسکن اخیر Shodan نشان می دهد که کشور ایران بعد از کشورهای چین، آرژانتین، اروگوئه و ایالات متحده، پنجمین کشوری می‌باشد که سرویس دهندگان UPnP بر روی اینترنت در دسترس می‌باشند و احتمال بهره‌برداری از آسیب‌پذیری ذکر شده بر روی آنها وجود دارد. این گزارش همچنین نشان می‌دهد اکثر تجهیزات مربوط به شرکت‌های ارتباطی مخابرات ایران و برخی از شرکت‌های خصوصی نظیر شاتل و پارس آنلاین می‌باشند. در بین محصولات آسیب‌پذیر نیز نام Avtech AVN801 network camera و Allegro RomPager به چشم می‌خورد. شکل ۱ این پراکندگی را نشان می دهد.




**شکل ۱) میزان پراکندگی دستگاهها با سرویس UPnP در سطح جهان**

# ۳ میزان تاثیرگذاری

یک مهاجم غیر مجاز از راه دور ممکن است بتواند از قابلیت UPnP SUBSCRIBE برای ارسال ترافیک به مقصدهای دلخواه خود سوء استفاده کرده و منجر به حملات گسترش‌یافته DDoS و استخراج داده (Exfilteration) شود. به طور کلی، تهیه UPnP از طریق اینترنت می‌تواند آسیب‌پذیری‌های امنیتی بیشتری را نسبت به مواردی که در این گزارش شرح داده شده است، ایجاد کند.

## ۳-۱ چه کسانی در معرض این آسیب‌پذیری قرار دارند

میلیاردها دستگاه UPNP در شبکه‌های محلی و نیز میلیون‌ها دستگاه UPnP در بستر اینترنت قرار دارند. CallStranger یک آسیب‌پذیری پروتکل است بنابراین تقریبا تمام دستگاه‌های UPnP (و احتمالا دستگاه‌های شما) باید بروزرسانی شوند. شما می‌توانید با استفاده از ابزار موجود در GitHub بررسی کنید که آیا دستگاه شما آسیب‌پذیر است یا خیر.

## ۳-۲ کاربران خانگی

انتظار نمی‌رود که کاربران خانگی مستقیما مورد هدف قرار گیرند. اگر دستگاه‌های در معرض اینترنت آنها دارای UPnP endpoints باشند، ممکن است دستگاه‌های آنها برای منبع حمله DDoS مورد استفاده قرار

گیرند. از ارائه دهنده سرویس‌های اینترنتی (ISP) خود بپرسید که آیا روتر شما در معرض آسیب‌پذیری CallStranger قرار دارد یا خیر. به UPnP endpoints منتقل نشوید.

## ۳-۳ ISP

ارائه دهندگان سرویس‌های اینترنتی یا ISP ها به بررسی پشته UPnP روترهای DSL/Cable خود نیاز دارند، از آنها بخواهید که در صورت آسیب‌پذیر بودن قابلیت SUBSCRIBE در دستگاه‌ها، آنها را بروزرسانی نمایند. ISPها می‌توانند دسترسی به پورت‌های شناخته شده‌ی UPnP Control & Eventing را در صورتیکه از طریق اینترنت قابل دسترسی باشند مسدود نمایند. آنها همچنین می‌توانند CPE را با کمک TR-069 مجددا تنظیم کنند.

## ۳-۴ فروشندگان دستگاه

بسته به مشخصات جدید UPnP در وب‌سایت OCF، باید پشته UPnP دستگاه خود را وصله نمایید. برخی از پشته‌های UPnP مانند miniupnp (بعد از سال ۲۰۱۱) آسیب‌پذیر نیستند.

## ۳-۵ شرکت

ممکن است فروشندگان، وصله دستگاه‌های UPnP را طولانی کنند، شرکت‌ها باید اقدامات خود را انجام دهند. شرکت‌ها باید بسته به رویکرد خود اقدامات لازم را بکار گیرند.

## ۳-۶ دستگاه‌های آسیب‌پذیر

دستگاه‌هایی که آسیب‌پذیری آنها تایید شده است عبارتند از:

- Windows 10 (All windows versions) - upnphost.dll 10.0.18362.719
- Xbox One- OS Version 10.0.19041.2494
- ADB TNR-5720SX Box (TNR-5720SX/v16.4-rc-371-gf5e2289 UPnP/1.0 BH-upnpdev/2.0)
- Asus ASUS Media Streamer
- Asus Rt-N11
- Belkin WeMo
- Broadcom ADSL Modems
- Canon Canon SELPHY CP1200 Printer
- Cisco X1000 - (LINUX/2.4 UPnP/1.0 BRCM400/1.0)
- Cisco X3500 - (LINUX/2.4 UPnP/1.0 BRCM400/1.0)
- D-Link DVG-N5412SP WPS Router (OS 1.0 UPnP/1.0 Realtek/V1.3)

- EPSON EP, EW, XP Series (EPSON_Linux UPnP/1.0 Epson UPnP SDK/1.0)
- HP Deskjet, Photosmart, Officejet ENVY Series (POSIX, UPnP/1.0, Intel MicroStack/1.0.1347)
- Huawei HG255s Router - Firmware HG255sC163B03 (ATP UPnP Core)
- NEC AccessTechnica WR8165N Router ( OS 1.0 UPnP/1.0 Realtek/V1.3)
- Philips 2k14MTK TV - Firmware TPL161E_012.003.039.001
- Samsung UE55MU7000 TV - Firmware T-KTMDEUC-1280.5, BT - S
- Samsung MU8000 TV
- TP-Link TL-WA801ND (Linux/2.6.36, UPnP/1.0, Portable SDK for UPnP devices/1.6.19)
- Trendnet TV-IP551W (OS 1.0 UPnP/1.0 Realtek/V1.3)
- Zyxel VMG8324-B10A (LINUX/2.6 UPnP/1.0 BRCM400-UPnP/1.0)

دستگاه‌هایی نیز که منتظر تایید آسیب‌پذیر بودن هستند عبارتند از:

- Dell B1165NFW
- LG Smartshare Media Application
- Netgear WNHDE111 Access Point
- Nokia HomeMusic Media Device
- Panasonic BB-HCM735 Camera
- Panasonic VL-MWN350 wireless doorphone
- Plutinosoft Dynamic UPnP stack
- Ruckus Zone Director Access Point
- Siemens CNE1000 Camera
- Sony Media Go Media application
- Stream What You Hear Stream What You Hear
- Toshiba TCC-C1 Media Device
- Ubiquiti UniFi Controller
- ZTE ZXV10 W300
- ZTE H108N

# ۴ راه‌حل‌ها

## ۴-۱ اعمال بروزرسانی

توصیه می‌شود تنظیمات به روز شده و ارائه شده توسط OCF پیاده‌سازی شود.

### ۴-۲ غیرفعال یا محدود کردن UPnP

پروتکل UPnP را در رابط‌های قابل دسترسی به اینترنت غیرفعال کنید. از سازندگان دستگاه خواسته شده است که قابلیت UPnP SUBSCRIBE را در پیکربندی پیش‌فرض خود غیرفعال کنند و از کاربران بخواهند تا صریحا با محدودیت‌های مناسب شبکه، SUBSCRIBE را فعال کنند تا میزان استفاده آن از یک شبکه محلی قابل اعتماد محدود شود.

### ۴-۳ IDS Signature

مدیران شبکه و ISPها می‌توانند یک signature را در تجهیزات لبه اتصال شبکه سازمان خود به اینترنت تعریف نمایند تا هرگونه درخواست غیرعادی SUBSCRIBE که به کاربرانشان می‌رسد را تشخیص دهند. به عنوان مثال امضای زیر برای Surricata IDS قابل استفاده می‌باشد:

```
alert http any any ->
![fd00::/8,192.168.0.0/16,10.0.0.0/8,172.16.0.0/12] any (msg:"UPnP
SUBSCRIBE request seen to external network VU#339275: CVE- 2020-12695
https://kb.cert.org "; content: "subscribe"; nocase; http_met hod;
sid:1367339275;)
```

## ۵ جمع بندی

درنهایت با توجه به اینکه این آسیب‌پذیری مربوط به یک پروتکل می باشد، زمان زیادی نیاز دارد که اصلاح و رفع شود. در حال حاضر پیشنهاد می گردد این آسیب‌پذیری را جدی گرفته و تا رفع کامل آن، سرویس UPnP را محدود و یا مسدود سازید. با توجه به گستردگی و اهمیت موضوع، پیشنهاد می‌شود کلیه مدیران و کارشناسان فناوری اطلاعات علی الخصوص شرکت‌های مذکور هر چه سریعتر نسبت به بررسی تنظیمات تجهیزات خود و مشتریانشان اقدام لازم را انجام دهند.

## ۶ منابع:

https://callstranger.com/
https://kb.cert.org/vuls/id/339275
https://www.shodan.io/search?query=upnp