BOLETÍN DE ALERTA

Boletín Nro.: 2020-16
Fecha de publicación: 09/06/2020
Tema: Vulnerabilidad en implementación de UPnP permitiría realizar ataques DDoS

Descripción:

Recientemente fue descubierta una vulnerabilidad que afecta al protocolo **Universal Plug and Play (UPnP)** cuando es utilizada la funcionalidad **SUBSCRIBE** que afecta a especificaciones anteriores a la fecha del **17/04/2020,** identificada y catalogada con el **CVE-2020-12695** de riesgo **crítico**, la vulnerabilidad también se conoce como **CallStranger.**

El fallo se da debido a que el valor de la función de retorno **Callback** del encabezado dentro de **UPnP SUBSCRIBE** puede ser controlado por un atacante no autenticado, ya que **UPnP** es un protocolo especialmente diseñado para ser utilizado en una **red de área local (LAN)** de confianza, por lo tanto no implementa forma alguna de autenticación o verificación, esto podría dar lugar a vulnerabilidades del tipo **SSRF (Server Side Request Forgery)**, vulneranbilidades que permitan realizar ataques **DDoS**, filtración de datos y otros comportamientos inusuales dentro de la red y que afectan a millones de dispositivos accesibles a través de internet compatibles con **UPnP.**

Impacto:

Esta vulnerabilidad podría permitir a un atacante remoto no autenticado, abusar de la funcionalidad **SUBSCRIBE** enviando grandes cantidades de datos a destinos arbitrarios accesibles a través de internet, llevando así a un ataque de **denegación de servicio distribuida (DDoS)**, también se podría sobrepasar la seguridad de la red con el fin de **extraer** datos confidenciales.

Solución y prevención:

- La **Open Connectivity Foundation (OCF)** ha actualizado la **especificación UPnP** con el fin de abordar este problema, se recomienda a los usuarios estar atentos a los canales de soporte de los fabricantes a la espera de la implementación de la nueva especificación **SUBSCRIBE.**
- Deshabilitar la funcionalidad **SUBSCRIBE** en su configuración por defecto y

configurarla explícitamente con las restricciones de red apropiadas para limitar el uso a la **red de área local (LAN).**

- Aplicar una nueva regla al **IDS (Sistema de Detección de Intruso), en caso de contar con uno.** La regla de ejemplo busca solicitudes **HTTP SUBSCRIBE** que provengan de una red externa. Los administradores de red y proveedores de servicios de internet podrían utilizarla para detectar solicitudes anómalas de **SUBSCRIBE** que lleguen a los usuarios:

```
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;)
```

Información adicional:

- http://www.callstranger.com/
- https://www.kb.cert.org/vuls/id/339275
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidad-implementacion-upnp
- https://www.helpnetsecurity.com/2020/06/09/cve-2020-12695/