INFORME SEMANAL

ACTIVIDADES GENERALES CONTEXTO GLOBAL

[COLCERT IS-0416-S15]

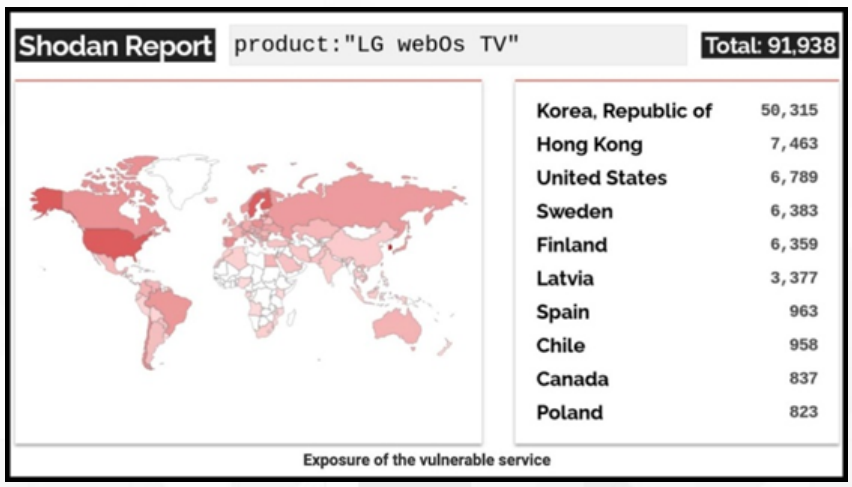
EVENTO	DESCRIPCIÓN	UBICACIÓN DEL EVENTO O ENTIDAD AFECTADA	ACTOR O DOMINIO AFECTADO
Vulnerabilidades LG	Posibles Exploits vienen instalándose en dispositivos de la marca y frente a dispositivos activos.	Global	LG

Impacto

Se han identificado cuatro vulnerabilidades en televisores inteligentes LG, que afectan a las versiones de WebOS 4-7. Estas vulnerabilidades permiten a los atacantes eludir la autorización, obtener acceso de root y tomar el control total del televisor. Más de 91,000 televisores inteligentes LG son vulnerables a estos ataques, con puntuaciones críticas de CVSS de 9.1. Alto Crítico.

Análisis tendencial

Los dispositivos inteligentes son vulnerables y se recomienda se recomienda realizar pruebas de seguridad regulares para identificar y corregir vulnerabilidades, evitar la explotación de éstas. El incremento en la utilización de dispositivos IoT conectados a redes públicas y privadas los hace objetivos atractivos para los ciberatacantes, lo que indica la necesidad de implementar controles de seguridad sólidos en todos los dispositivos del hogar inteligente.



FUENTES:

https://secalerts.co/news/more-than-91-000-lg-smart-tvs-open-to-remote-attack/6vV9PLxb500tESGXyZZuy7

Monitoreo del espacio cibernético o alertas

Las versiones del sistema operativo afectados incluyen webOS 4.9.7 - 5.30.40, webOS 5.5.0 - 04.50.51 y webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50.

Proyección

•LG ha solucionado las siguientes vulnerabilidades de seguridad en sus televisores inteligentes:

•webOS 4.9.7 - 5.30.40 ejecutándose en LG43UM7000PLA

•webOS 5.5.0 - 04.50.51 ejecutándose en OLED55CXPUA

•webOS 6.3.3-442 (kisscurl-kinglake) - 03.36.50 ejecutándose en OLED48C1PUB

•webOS 7.3.1-43 (mullet-mebin) - 03.33.85 ejecutándose en OLED55A23LA

FUENTES:

https://www.techradar.com/televisions/lg-fixes-worrying-security-vulnerabilities-on-some-smart-tvs-check-if-your-model-is-among-them

INFORME SEMANAL

ACTIVIDADES RELEVANTES CONTEXTO GLOBAL

[COLCERT IS-0416-S15]

EVENTO	DESCRIPCIÓN	UBICACIÓN DEL EVENTO O ENTIDAD AFECTADA	ACTOR O DOMINIO AFECTADO
Exploit para Kernel de Linux	Utiliza un mecanismo similar a los errores Spectre anteriores, al aprovechar las tiendas especulativas que conducen a los desbordamientos de búfer.	Global	El documento mencionado es CVE-2024-2201

Impacto

Se ha descubierto el primer exploit nativo de Spectre v2 contra el kernel de Linux en sistemas Intel, llamado Inyección Nativa de Historial de Ramas (BHI). Este exploit puede utilizarse para filtrar memoria del kernel a una velocidad de 3.5 kB/seg al eludir las mitigaciones existentes de Spectre v2/BHI. Medio Crítico.

Análisis tendencial

Las técnicas de mitigación existentes son insuficientes para detener la explotación de BHI,un atacante no autenticado puede aprovechar esta vulnerabilidad para filtrar memoria privilegiada de la CPU. Este descubrimiento resalta la importancia de continuo ajuste de medidas de seguridad y la mitigación de vulnerabilidades en los sistemas informáticos, especialmente en entornos donde se manejan datos sensibles y privilegiados.

Monitoreo del espacio cibernético o alertas

El exploit afecta a todos los sistemas Intel susceptibles a BHI y puede ser utilizado por atacantes para influir en los caminos de ejecución especulativa y extraer datos sensibles de diferentes procesos.

Proyección

La constante secuencia de ataques especulativos de buffer overflow ha resultado en la identificación y monitoreo de la vulnerabilidad Spectre 1.1, conocida como CVE-2018-3693. En un artículo escrito por Vladimir Kiriansky y Carl Waldspurger se explican los detalles de este nuevo riesgo".This vulnerability utilizes a mechanism akin to previous Spectre flaws, taking advantage of speculative operations that lead to the mentioned buffer overflows. Además, se le conoce como "BoundsCheck Bypass Store" o BCBS simplemente para diferenciarla de otras vulnerabilidades de Spectre.

FUENTES:

https://bugzilla.redhat.com/show_bug.cgi?id=2268118

https://sensorstechforum.com/google-chrome-mitigates-spectre-vulnerability-via-site-isolation/

https://sensorstechforum.com/cve-2018-3693-new-spectre-1-1-vulnerability-emerges/

INFORME SEMANAL

ACTIVIDADES RELEVANTES CONTEXTO GLOBAL

[COLCERT IS-0416-S15]

EVENTO	DESCRIPCIÓN	UBICACIÓN DEL EVENTO O ENTIDAD AFECTADA	ACTOR O DOMINIO AFECTADO
Ciberataque	Brecha de datos ocasionada contra el ISP AT&T	Global	AT&T

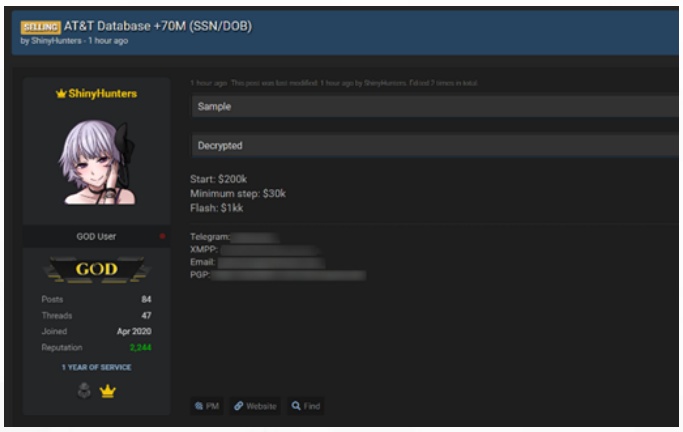
Impacto

En el documento se mencionan varias noticias relacionadas con la seguridad cibernética y la privacidad de los usuarios. Estos eventos tienen un impacto significativo en la confianza de los usuarios y en la percepción de la seguridad de los servicios y productos digitales. Bajo Crítico

Análisis tendencial

Las acciones tomadas por empresas y agencias gubernamentales en respuesta a estas noticias pueden influir en la forma en que se abordan los riesgos de seguridad cibernética en el futuro y en cómo se protegen los datos sensibles de los usuarios.

.



FUENTES:

https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/

https://www.bleepingcomputer.com/news/security/att-now-says-data-breach-impacted-51-million-customers/

https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/

Monitoreo del espacio cibernético o alertas

Bleeping computing expuso la línea de tiempo de la brecha y posible ciberataque efectuado.

Proyección

En agosto de 2021, AT&T, el principal proveedor de servicios de comunicaciones, fue víctima de un ciberataque por parte de ShinyHunters, quien declaró tener acceso a una base de datos con información personal de 70 millones de clientes.

ShinyHunters comenzó a vender la presunta base de datos en un foro de piratería el día de ayer, iniciando en $200,000 y aceptando ofertas cada vez mayores de $30,000.

El mes pasado, durante un incidente en el que otro actor de amenazas llamado 'MajorNelson' filtró toda la base de datos en un foro de piratería, AT&T reiteró a BleepingComputer que los datos no tenían su origen en la empresa y que sus sistemas no habían sido comprometidos.

INFORME SEMANAL

ACTIVIDADES RELEVANTES CONTEXTO GLOBAL

[COLCERT IS-0416-S15]

EVENTO	DESCRIPCIÓN	UBICACIÓN DEL EVENTO O ENTIDAD AFECTADA	ACTOR O DOMINIO AFECTADO
Palo Alto Networks	Vulnerabilidad de inyección de comandos del sistema operativo en GlobalProtect	Global	GlobalProtect del software PAN-OS de Palo Alto Networks

Impacto

Representa un riesgo crítico, con una puntuación de gravedad de 10, indicando un potencial de daño extremo debido a la capacidad de ejecución de comandos arbitrarios con privilegios de root por parte de atacantes. No requiere interacción del usuario ni privilegios especiales para ser explotada, lo que aumenta significativamente su peligrosidad y facilita su automatización. Afecta a ciertas versiones de PAN-OS, aunque en el interín, se han proporcionado medidas de mitigación para proteger a los usuarios contra posibles ataques que exploten esta vulnerabilidad.

Análisis tendencial

La creciente ola de ataques severos que no necesitan interacción del usuario resalta la imperiosa necesidad de reforzar la seguridad en el software de infraestructura crítica. La vulnerabilidad CVE-2024-3400 permite a los atacantes ejecutar comandos como root, lo cual enfatiza la importancia de actualizar y monitorear de forma continua herramientas de seguridad. Palo Alto Networks ha reaccionado rápidamente, preparando parches para las versiones afectadas, demostrando una actitud proactiva en la gestión de ciberseguridad. No obstante, el hecho de que ya se estén llevando a cabo ataques aprovechando esta vulnerabilidad, destaca la constante necesidad de estar vigilantes y adaptarse ante los actores de amenazas que están en evolución continua

FUENTES:

- security.paloaltonetworks.com - OS Command Injection Vulnerability in GlobalProtect
- csirt.gob.cl - Palo Alto Networks PAN-OS - Vulnerabilidades
- vuldb.com - Palo Alto Networks PAN-OS GlobalProtect escalada de
- portal.cci-entel.cl - Vulnerabilidad crítica afecta a PAN-OS de Palo Alto
- linkedin.com - Falla crítica de PAN-OS en Palo Alto Networks bajo ataque
- incibe.es - CVE-2024-3400

Monitoreo del espacio cibernético o alertas

Esta vulnerabilidad a la cual la tecnología ML de PAN-OS de Palo Alto Networks, se encentra expuesta, evidencian los riesgos a los que enfrentan las infraestructuras de TI. Esta falla, permite la inyección de comandos mediante GlobalProtect, la cual puede ser utilizada por atacantes sin autenticación para ejecutar código con privilegios de root. Es vital realizar monitoreo activo, aplicar parches de seguridad de manera oportuna, implementar bloqueos específicos de ID de amenazas y proteger las interfaces críticas. Además, prestar atención a los análisis de seguridad y seguimientos de explotaciones activas para prevenir ataques y reducir riesgos.

Proyección

Esta vulnerabilidad, calificada con la máxima criticidad, destaca el aumento en la gravedad y complejidad de los ciberataques a infraestructuras críticas. La fácil explotación de esta vulnerabilidad sin interacción del usuario sugiere un probable incremento en los intentos de ataque, lo que demanda respuestas urgentes y mejoras en las medidas de seguridad como la detección proactiva y parches automáticos. Las organizaciones también deberían mejorar sus sistemas de telemetría y monitorización para prevenir futuros ataques.

.