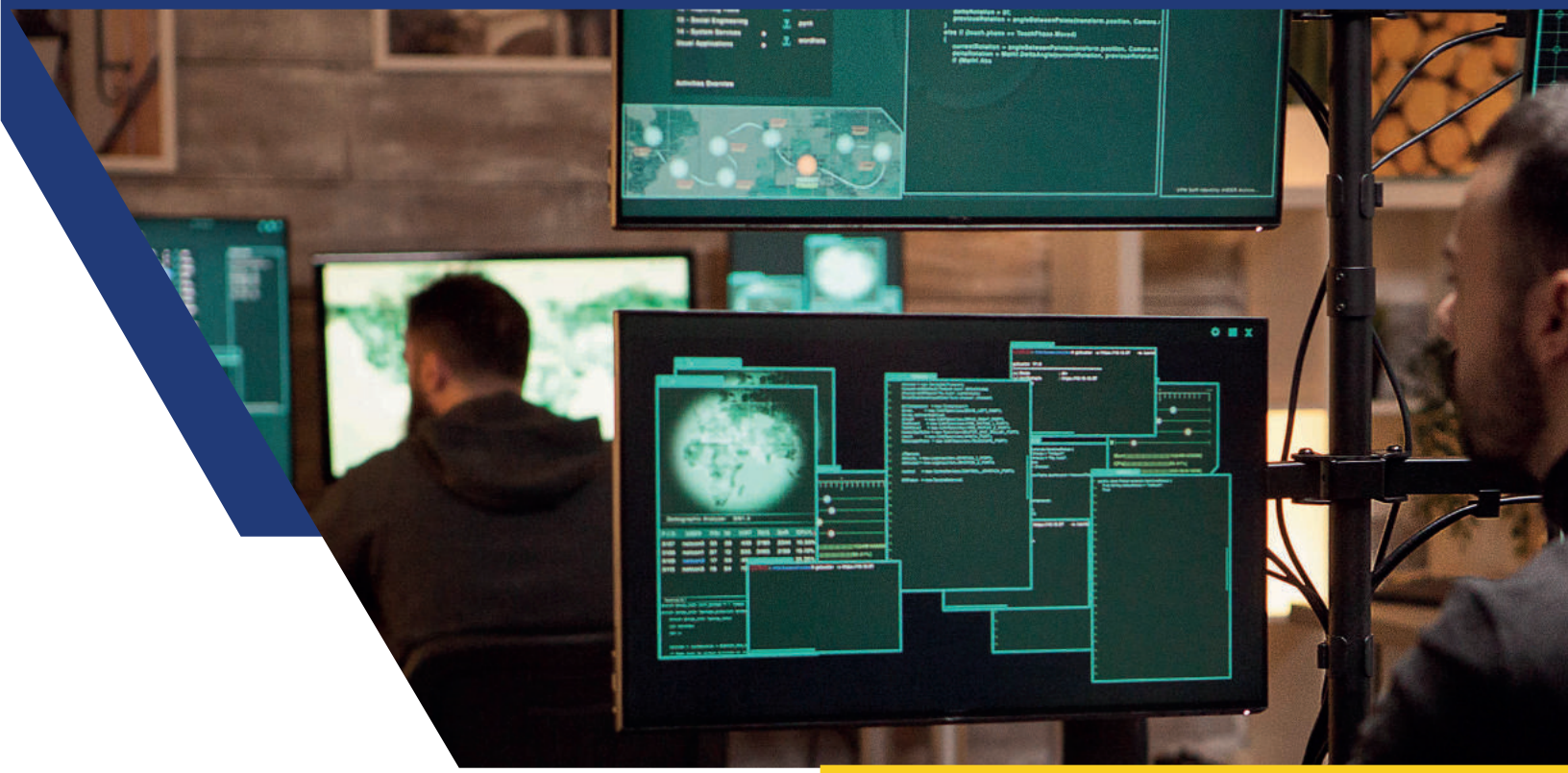
CENTAURI
TECHNOLOGIES CORPORATION

VULNERABILIDADES QUE DAN DE QUE HABLAR

JULIO 2022



CVE-2022-34918: Linux kernel: Netfilter buffer overflow

CVSS: 3: 7.8

Se descubrió una vulnerabilidad en el kernel de Linux versión 5.18.9. Un atacante local podría generar un buffer overflow en el subsistema Netfilter generando una entrada incorrecta en nft_set_elem_init para escalar privilegios.

Mitigación: Esto se puede arreglar en nft_setelem_parse_data en net/netfilter/nf_-tables_api.c.

Fuentes: https://nvd.nist.gov/vuln/detail/CVE-2022-34918
https://access.redhat.com/security/cve/cve-2022 34918#:~:text=Description, than%20CVE%2D2022%2D32250.

CVSS: 3: 9.8

CVE-2022-2274

Corrupción de memoria heap con la operación de clave privada RSA

La versión OpenSSL 3.0.4 introdujo un error grave en la implementación de RSA para arquitecturas X86_64 compatibles con las instrucciones AVX512IFMA.
Este problema hace que la implementación de RSA con claves privadas de 2048 bits sea incorrecta en dichas máquinas. La corrupción de la memoria permite a un atacante generar una ejecución remota de código en la máquina que realiza el cálculo.

Mitigación: Los usuarios de la versión OpenSSL 3.0.4 deben actualizar a OpenSSL 3.0.5.

Fuentes: https://www.openssl.org/news/secadv/20220705.txt

https://www.cvedetails.com/cve/CVE-2022-2274/

CVSS: 3: 7.5

CVE-2022-32230: Vulnerabilidad de denegación de servicio en Windows SMB

Explotando una vulnerabilidad sobre el protocolo SMBv3 se puede generar un ataque de denegación de servicios sobre el sistema. Un atacante puede provocar un bloqueo de pantalla azul de la muerte (BSOD) del kernel. Este ataque requiere autenticación, excepto en el caso de los controladores de dominio de dominio.

Mitigación: Esta vulnerabilidad se corrigió en las actualizaciones de seguridad de mayo de 2022.

Fuente: https://nvd.nist.gov/vuln/detail/CVE-2022-32230

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-32230

CVSS: 6.5

CVE-2022-20859: Vulnerabilidad de control de acceso de productos de Cisco Unified Communications.

Una vulnerabilidad en los gestores Disaster Recovery framework of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), y Cisco Unity Connection podría permitir que un atacante que se encuentre autenticado realice ciertas acciones privilegiadas, incluso si este cuenta con privilegios de solo lectura. Esta vulnerabilidad es resultado de comprobaciones de control de acceso insuficientes en el dispositivo afectado.

Fuente: https://tools.cisco.com/security/center/content/CiscoSecuryAdvisory/cisco-sa-ucm-access-dMKvV2DY

TOP 25
DE LAS DEBILIDADES más peligrosas en software

Durante el mes de junio fue liberado por mitre el top 25 de las debilidades más peligrosas en el software. Este top sale del análisis de los CVE registrados en los últimos 2 años calendario. De aquí se puede obtener un panorama para direccionar la aplicación de controles; a continuación, compartimos las 10 debilidades más comunes.
Para más información y la lista completa dirigirse a:
https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

RANK

1 2 3 4 5 6 7 8 9 10

1 CWE-787

Out-of-bounds Write

2 CWE-79

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

3 CWE-89

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

4 CWE-20

Improper Input Validation

RANK

1 2 3 4 5 6 7 8 9 10

5 CWE-125

Out-of-bounds Read

6 CWE-78

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

7 CWE-416

Use After Free

8 CWE-20

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

9 CWE-352

Cross-Site Request Forgery (CSRF)

10 CWE-434

Unrestricted Upload of File with Dangerous Type

Considérenos el 911 de tecnología de información

CENTAURI
TECHNOLOGIES CORPORATION

info@centauritech.com

www.centauritech

Tel: (+507) 317-1217

Centauri Technologies Corporation