I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- RANSOMWARE GUNRA EXPLOTA VULNERABILIDADES CRÍTICAS EN FORTINET - figura referencial

Una nueva campaña de ataque atribuida al grupo de Ransomware Gunra está dirigida contra dispositivos Fortinet. La explotación de las vulnerabilidades CVE-2024-55591 y CVE-2025-24472 puede permitir a un atacante evadir los mecanismos de autenticación multifactor (MFA), obtener privilegios elevados, potencialmente de superadministrador y acceder de forma no autorizada a la infraestructura afectada, lo que podría permitir comprometer posteriormente redes y recursos empresariales

III. INTRODUCCIÓN

El grupo de Ransomware Gunra apareció por primera vez en 2025 estableciéndose como un operador significativo en el mundo del ransomware, opera bajo el modelo de ransomware como servicio (RaaS), donde los desarrolladores del malware ponen su infraestructura a disposición de sus afiliados para que ejecuten los ataques. Emplea también una estrategia de doble extorsión, que combina el cifrado de los sistemas (a archivos .gunra) con la exfiltración de información sensible, amenazando con publicar los datos sustraídos si no se efectúa el pago del rescate.

Agencias como FBI y CISA (Cybersecurity and Infrastructure Security Agency) en Estados Unidos y NIS (National Intelligence Service) y NPA (National Police Agency) en Corea del Sur, han reportado actividad sostenida por parte del Grupo de Ransomware Gunra y advierten sobre su expansión hacia organizaciones de diferentes sectores. Entre los objetivos identificados se encuentran entidades de salud, servicios financieros, manufactura, transporte, servicios públicos y gobierno. Esta actividad incrementa el riesgo para organizaciones que mantienen dispositivos Fortinet vulnerables o interfaces de administración expuestas a Internet, especialmente cuando no se han aplicado las actualizaciones de seguridad correspondientes.

Las vulnerabilidades explotadas por el grupo de Ransomware Gunra corresponden a fallas de omisión de autenticación en ambos productos de Fortinet FortiOS y FortiProxy.

CVE-2024-55591 es una vulnerabilidad que permitiría que un atacante remoto no autenticado obtenga privilegios de superadministrador mediante el envío de solicitudes especialmente diseñadas al componente Node.js, utilizado para procesar las comunicaciones a través de WebSocket. La vulnerabilidad está asociada a la CWE-288 (Authentication Bypass Using an Alternate Path or Channel).

CVE-2025-24472 es una vulnerabilidad que permitiría que un atacante remoto no autenticado, con conocimiento previo de los números de serie de los dispositivos upstream y downstream (identificadores únicos asignados a cada dispositivo Fortinet), obtenga privilegios de superadministrador en el dispositivo downstream, siempre que la función Security Fabric esté habilitada, mediante solicitudes de proxy CSF especialmente diseñadas.

Mediante la explotación de ambas vulnerabilidades, los atacantes pueden dirigirse contra dispositivos firewall y VPN expuestos a Internet. Una vez comprometidos estos dispositivos, pueden utilizarlos como punto de acceso a la infraestructura interna, desplegar el ransomware y exfiltrar información sensible antes de proceder con el cifrado de los sistemas.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2024-55591 tiene un vector de ataque tipo RED CVSS: 3.1/AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: H/A: H con nivel de severidad 9.8 CRÍTICO.

La vulnerabilidad CVE-2025-24472 tiene un vector de ataque tipo RED CVSS: 3.1/AV: N/AC: L/PR: N/UI: N/S: U/C: H/I:H/A:H con nivel de severidad 9.8 CRÍTICO.

El grupo de Ransomware Gunra ha explotado vulnerabilidades críticas en dispositivos Fortinet FortiOS y FortiProxy expuestos a Internet (CVE-2024-55591 y CVE-2025-24472) para obtener acceso inicial a los entornos comprometidos. Una vez dentro de la infraestructura, los atacantes demostraron una elevada capacidad para establecer mecanismos de persistencia mediante la creación de una nueva cuenta de usuario denominada forticloud-sync, con cuyo nombre buscaban pasar desapercibido entre los procesos legítimos del sistema y los servicios de sincronización en la nube. Asimismo, lograron desplazarse lateralmente por la red, recurriendo principalmente a técnicas orientadas a eludir los mecanismos de autenticación.

En uno de los incidentes analizados, los atacantes obtuvieron acceso a una cuenta de administrador de un dispositivo VPN SSL (Secure Socket Layer) mediante el uso de credenciales predeterminadas, aprovechando la ausencia de políticas de bloqueo tras múltiples intentos fallidos de autenticación. Posteriormente, establecieron canales de comunicación entre los sistemas comprometidos y un servidor externo bajo su control mediante la instalación de la herramienta OpenSSH, utilizada para crear túneles de comunicación remotos.

Asimismo, consiguieron eludir de forma persistente la autenticación multifactor (MFA) mediante la modificación de los archivos responsables del procesamiento de la autenticación en el servidor del portal corporativo de infraestructura de escritorios virtuales (VDI), lo que les permitió mantener el acceso a los sistemas comprometidos.

Se detalla el TTP:

Táctica	Identificación	Técnica
Acceso inicial	T1190	Aprovechamiento de FortiOS/Forti-Proxy (CVE-2024-55591, CVE-2025-24472) para crear una cuenta de superusuario en FortiCloud-Sync.
Cuentas válidas	T1078	Aprovechamiento de cuentas de administrador de SSL-VPN no utilizadas
Control exclusivo	T1668	Control exclusivo: Robo de claves de cifrado simétrico del sistema Hiware

Táctica	Identificación	Técnica
Aprovechamiento de servicios remotos	T1210	Transferencia de datos mediante Impacket (psexec.py, smbclient.py) y túneles OpenSSH
Extracción de credenciales del sistema operativo: NTDS	T1003.003	Uso de secretsdump.py para extraer información relacionada con la autenticación en sistemas Windows.
Modificación del proceso de autenticación: MFA	T1556.006	Eludir la autenticación multifactorial mediante modificaciones en el portal VDI
Datos del almacenamiento en la nube	T1530	Extracción de datos de OneDrive/ SharePoint
Exfiltración al almacenamiento en la nube	T1567.002	Utilizando RClone, 7-Zip y FileZilla para subir archivos a Mega
Inhibición de la recuperación del sistema:	T1490	Eliminación de shadow copies
Destrucción de datos	T1485	Destrucción de copias de seguridad: implementación de ransomware (Chacha20/RSA-4096)

Tabla 1.- TTP - RANSOMWARE GUNRA EXPLOTA VULNERABILIDADES CRÍTICAS EN FORTINET

V. IMPACTO

Fabricante	Producto	Componente afectado	Versiones afec-tadas	Plataforma/SO
Fortinet	FortiOS	Módulo Node.js WebSocket	7.0.0 – 7.0.16	FortiOS
Fortinet	FortiProxy	Módulo Node.js WebSocket	7.0.0 – 7.0.19	FortiProxy
Fortinet	FortiProxy	Módulo Node.js WebSocket	7.2.0 – 7.2.12	FortiProxy

Tabla 2.- Productos afectados – CVE-2024-55591 - RANSOMWARE GUNRA EXPLOTA VULNERABILIDADES CRÍTICAS EN FORTINET

Fabricante	Producto	Componente afectado	Versiones afec-tadas	Plataforma/SO
Fortinet	FortiOS	Security Fabric / CSF Proxy	7.0.0 – 7.0.16	FortiOS
Fortinet	FortiProxy	Security Fabric / CSF Proxy	7.0.0 – 7.0.19	FortiProxy
Fortinet	FortiProxy	Security Fabric / CSF Proxy	7.2.0 – 7.2.12	FortiProxy

Tabla 3.- Productos afectados – CVE-2025-24472 - RANSOMWARE GUNRA EXPLOTA VULNERABILIDADES CRÍTICAS EN FORTINET

VI. INDICADORES DE COMPROMISO

Tipo	Indicador de compromiso
Fortinet	Creación inesperada de cuentas con privilegios de administrador o superadministrador.
Fortinet	Modificaciones no autorizadas en configuraciones de FortiOS/FortiProxy.
Fortinet	Solicitudes anómalas dirigidas a interfaces administrativas, WebSocket o CSF.
Acceso	Conexiones VPN o accesos administrativos desde direcciones IP no reconocidas.
Exfiltración	Transferencias de grandes volúmenes de información desde la red corporativa.
Movimiento lateral	Conexiones sospechosas desde el firewall comprometido hacia sistemas internos.
Gunra	Archivos cifrados asociados a la actividad del ransomware Gunra.
Impacto	Cifrado anómalo de archivos o eliminación de mecanismos de recuperación.

Tabla 4.- Indicadores de Compromiso - RANSOMWARE GUNRA EXPLOTA VULNERABILIDADES CRÍTICAS EN FORTINET

VII. RECOMENDACIONES:

- Actualizar FortiOS y FortiProxy a las versiones corregidas y soportadas por el fabricante, priorizando los dispositivos expuestos directamente a Internet.
- Verificar el inventario de dispositivos FortiGate y FortiProxy para identificar aquellos que ejecuten versiones afectadas por las vulnerabilidades CVE-2024-55591 y CVE-2025-24472.
- Restringir el acceso a las interfaces de administración desde Internet, permitiendo únicamente conexiones provenientes de redes administrativas o direcciones IP autorizadas.
- Implementar autenticación multifactor (MFA) para las cuentas administrativas y aplicar el principio de mínimo privilegio.
- Los equipos de seguridad deben vigilar la presencia de cuentas no autorizadas, como forticloud-sync y detectar cualquier uso sospechoso de las herramientas de Impacket.
- Archivos cifrados con extensiones asociadas al ransomware Gunra.
- Revisar los registros de autenticación, administración y actividad de los dispositivos afectados, prestando especial atención a accesos inusuales, intentos de autenticación fallidos y conexiones desde direcciones IP desconocidas.

- Monitorear los dispositivos mediante herramientas SIEM, EDR o XDR, estableciendo alertas ante actividades administrativas anómalas.
- Verificar la integridad de las configuraciones después de aplicar las actualizaciones, incluyendo cuentas administrativas, políticas de firewall, objetos de red y configuraciones de acceso remoto.
- Realizar una búsqueda retrospectiva de indicadores de compromiso (IoC) en los registros disponibles para determinar si los dispositivos afectados presentan evidencia de explotación o acceso no autorizado.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

THE HACKER NEWS (2026). Gunra Ransomware Exploits Fortinet FortiOS, FortiProxy Flaws to Breach Networks. https://thehackernews.com/2026/08/gunra-ransomware-exploits-fortinet-and.html

DIARIOBITCOIN (2026). Agencias federales advierten sobre el ransomware Gunra y su explotación de fallos en Fortinet. https://www.diariobitcoin.com/noticias/agencias-federales-advierten-sobre-el-ransomware-gunra-y-su-explotacion-de-fallos-en-fortinet/

SOC PRIME (2026). Gunra Ransomware Uses Multithreaded ChaCha20 Encryption. https://socprime.com/active-threats/gunra-ransomware-uses-multithreaded-chacha20-encryption/

INFOSECURITY MAGAZINE (2026). Gunra Ransomware Exploits Fortinet Flaws. https://www.infosecurity-magazine.com/news/gunra-ransomware-fortinet-flaws/