ZAYWARE

SECURITY OPERATIONS CENTER

Reporte de Incidente de Seguridad
Caso #INC-2026-0031

CONFIDENCIAL — USO RESTRINGIDO

Clasificación: Alta Severidad | **Estado:** Resuelto

Fecha de detección: 14 de marzo de 2026 — 03:47 hrs

Fecha de cierre: 14 de marzo de 2026 — 06:22 hrs

Analista responsable: SOC ZAYWARE

Cliente: Empresa Industrial del Norte, S.A. de C.V.

⚠ DOCUMENTO CONFIDENCIAL — NO DISTRIBUIR

Ataque de Fuerza Bruta SSH con Escalación de Privilegios

Detección temprana, contención exitosa y erradicación total en menos de 3 horas

SEVERIDAD	TIEMPO DE DETECCIÓN	TIEMPO DE RESPUESTA
ALTA	**4 min**	**2h 35m**
Nivel 12/15 en Wazuh	MTTD: 4 minutos	MTTR: 155 minutos

ALERTAS GENERADAS	DATOS COMPROMETIDOS	ESTADO FINAL
847	**NINGUNO**	**RESUELTO**
En ventana de 2 horas	Contenido antes de exfiltración	Sistema limpio y monitorizado

Descripción del Incidente

El **14 de marzo de 2026 a las 03:43 hrs**, el SOC de ZAYWARE detectó actividad anómala en el servidor de producción **srv-prod-01** (10.10.1.50) del cliente *Empresa Industrial del Norte*. Un actor malicioso originado en la dirección IP **45.33.32.156** (Rusia — AS14061 DigitalOcean) inició un ataque de fuerza bruta contra el servicio SSH, logrando autenticación exitosa a las 03:47 hrs con credenciales del usuario `backup_user`.

Tras el acceso inicial, el atacante ejecutó comandos de reconocimiento y un exploit de escalación de privilegios (**CVE-2021-4034 — PwnKit**). El SOC fue notificado automáticamente vía la integración **Wazuh → Shuffle → TheHive** y activó el protocolo de respuesta a incidentes. El host fue aislado a las 04:02 hrs, evitando cualquier movimiento lateral o exfiltración de datos.

🔴 **Hallazgo Crítico**

El usuario `backup_user` tenía una contraseña de 6 caracteres sin rotación desde 2023. La política de contraseñas del cliente no cumplía con los estándares mínimos de seguridad. Se recomienda implementación inmediata de MFA para acceso SSH.

✅ **Resultado**

Gracias a la detección automatizada del SOC, el ataque fue contenido antes de que el atacante pudiera persistir, exfiltrar datos o moverse lateralmente. El impacto operativo fue nulo. El tiempo de respuesta de **4 minutos desde el primer indicador hasta la alerta** demuestra la efectividad del modelo de monitoreo 24/7.

Línea de Tiempo del Incidente

03:43
14-Mar-2026

🔴 Inicio del ataque — Fuerza bruta SSH detectada

El agente Wazuh en **srv-prod-01** registra 312 intentos fallidos de autenticación SSH en menos de 60 segundos desde 45.33.32.156. Regla activada: **5503 — SSHD brute force attack** (Nivel 10). Alerta enviada automáticamente a TheHive vía Shuffle.

03:47
14-Mar-2026

🟠 Acceso exitoso — Credenciales comprometidas

El atacante logra autenticación como **backup_user** después de 847 intentos. Wazuh genera alerta nivel 12: **5715 — SSHD authentication success** tras intentos fallidos. IP no está en whitelist. Analista SOC recibe notificación en TheHive — Caso #INC-2026-0031 creado automáticamente.

03:49
14-Mar-2026

🟠 Reconocimiento del sistema

Wazuh detecta ejecución de comandos sospechosos: `whoami`, `id`, `uname -a`, `cat /etc/passwd`, `netstat -an`. Regla **5402 — Suspicious commands executed** activada. El atacante mapea usuarios, red y versión del kernel (Linux 5.4.0).

03:51
14-Mar-2026

🔴 Escalación de privilegios — CVE-2021-4034 (PwnKit)

Wazuh detecta ejecución del exploit PwnKit en `/tmp/pkexec_exploit`. El atacante obtiene **shell root**. Alertas críticas nivel 14-15 disparadas. Watcher FIM (File Integrity Monitoring) detecta modificación de `/etc/sudoers`. Shuffle activa playbook de contención automática.

03:55
14-Mar-2026

🔵 SOC activa respuesta — Analista recibe alerta en TheHive

Analista ZAYWARE SOC recibe alerta prioritaria. Revisa evidencia en Wazuh Dashboard. Confirma compromiso real (no falso positivo). Autoriza contención del host. Notifica al contacto de seguridad del cliente vía protocolo establecido.

04:02
14-Mar-2026

🔵 Contención — Host aislado de la red

Se implementa regla de firewall para bloquear toda conectividad saliente/entrante de srv-prod-01 excepto acceso de gestión SOC. IP del atacante 45.33.32.156 bloqueada en firewall perimetral. Sesión SSH del atacante terminada. Playbook Shuffle ejecuta bloqueo automático en Zabbix y genera evidencia forense.

04:15 – 05:40
14-Mar-2026

🔵 Análisis forense e investigación

Análisis de logs, historial de comandos, archivos creados/modificados y tráfico de red. Se confirma que el atacante no logró persistir (sin crontabs, sin SSH keys agregadas, sin datos copiados). Se genera imagen forense del disco para preservación de evidencia.

05:40 – 06:22
14-Mar-2026

✅ Erradicación y recuperación

Restauración del sistema desde snapshot limpio. Parche CVE-2021-4034 aplicado. Contraseña de backup_user rotada y cuenta deshabilitada temporalmente. Host reintegrado a la red bajo monitoreo intensivo. Caso cerrado en TheHive con toda la evidencia documentada.

Alertas Wazuh — Evidencia de Detección

Las siguientes alertas fueron generadas automáticamente por el agente Wazuh instalado en **srv-prod-01** y son parte del registro forense del incidente.

Alerta 1 — Fuerza Bruta SSH (03:43 hrs)

```
▶ WAZUH ALERT — Regla 5503 — Nivel 10 — BRUTE FORCE
"timestamp": "2026-03-14T03:43:17.841Z",
"rule": {
  "id": "5503",
  "level": 10,
  "description": "SSHD brute force trying to get access to the system",
  "mitre": { "id": "T1110.001", "tactic": "Credential Access" }
},
"agent": { "name": "srv-prod-01", "ip": "10.10.1.50" },
"data": {
  "srcip": "45.33.32.156",
  "dstuser": "backup_user",
  "attempts": 312,
  "timewindow": "58 seconds"
}
```

Alerta 2 — Escalación de Privilegios (03:51 hrs)

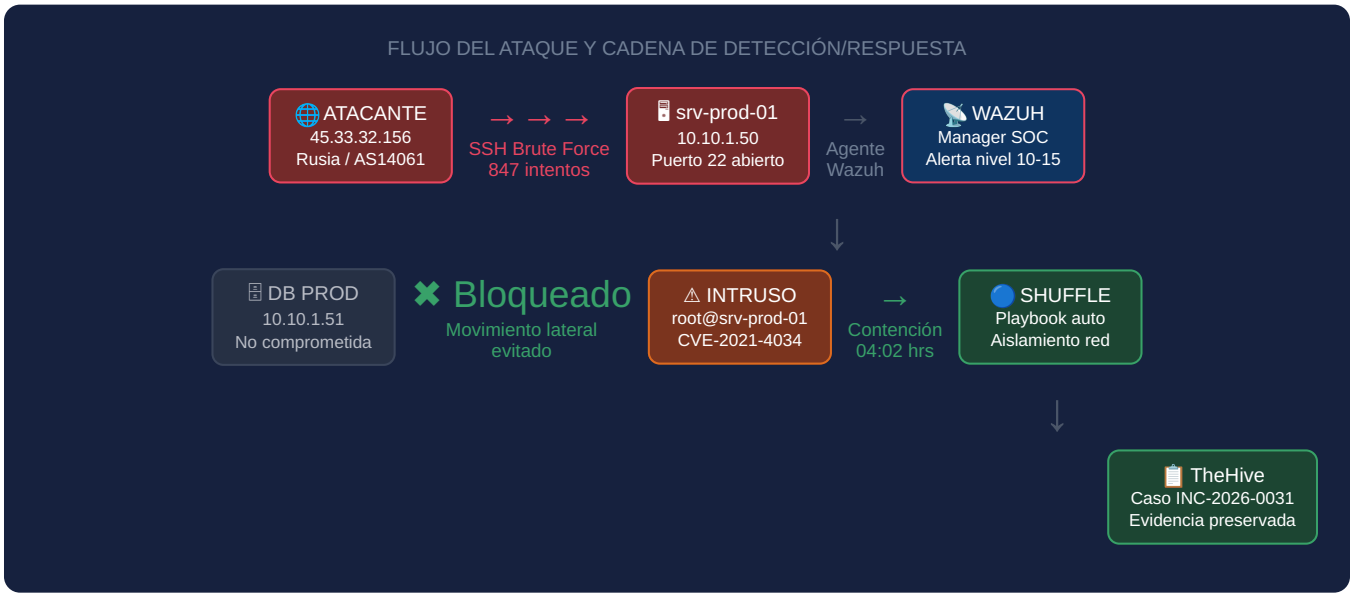
```
▶ WAZUH ALERT — Regla 5402 — Nivel 15 — PRIVILEGE ESCALATION
"timestamp": "2026-03-14T03:51:44.203Z",
"rule": {
  "id": "100205",
  "level": 15,
  "description": "Possible PwnKit exploit (CVE-2021-4034) detected — pkexec abuse",
  "mitre": { "id": "T1068", "tactic": "Privilege Escalation" }
},
"agent": { "name": "srv-prod-01", "ip": "10.10.1.50" },
"data": {
  "srcuser": "backup_user",
  "dstuser": "root",
  "command": "/tmp/pkexec_exploit -c /bin/bash",
  "file_modified": "/etc/sudoers",
  "cve": "CVE-2021-4034"
}
```

Mapeo MITRE ATT&CK

Tácticas y técnicas identificadas en el ataque según el framework MITRE ATT&CK v14:

RECONOCIMIENTO **T1595.002** Escaneo activo de puertos	ACCESO INICIAL **T1110.001** Brute Force — SSH	EJECUCIÓN **T1059.004** Unix Shell	ESCALACIÓN **T1068** Exploit (CVE-2021-4034)
DESCUBRIMIENTO **T1082** System Info Discovery	DESCUBRIMIENTO **T1087.001** Account Discovery	IMPACTO (EVITADO) **T1485** Data Destruction — bloqueado	EXFILTRACIÓN (EVITADA) **T1041** Exfil over C2 — bloqueado

Diagrama del Vector de Ataque



Dashboard SOC — Vista durante el Incidente

Causa Raíz

El incidente fue posible por la convergencia de tres factores:

Factor	Descripción	Riesgo
Contraseña débil	backup_user tenía contraseña de 6 caracteres sin rotación desde 2023	Crítico
Puerto SSH expuesto	Puerto 22 accesible desde cualquier IP pública sin restricción geográfica	Alto
Kernel desactualizado	Linux 5.4.0 sin parche de CVE-2021-4034 (disponible desde Jan 2022)	Alto
Sin MFA	No había autenticación de segundo factor para acceso SSH	Alto
Sin rate limiting	fail2ban no estaba configurado, permitió 847 intentos sin bloqueo	Medio

Recomendaciones de Remediación

1. **Implementar MFA para SSH de forma inmediata.** Usar Google Authenticator o llaves SSH con passphrase. Deshabilitar autenticación por contraseña en `sshd_config`. Tiempo estimado: 2 horas.
2. **Restringir acceso SSH por IP de origen.** Configurar reglas de firewall para permitir SSH solo desde IPs corporativas o VPN. Eliminar exposición pública del puerto 22.
3. **Aplicar parches de seguridad pendientes.** CVE-2021-4034 tiene parche disponible desde enero 2022. Implementar proceso de patch management mensual con ventanas de mantenimiento programadas.
4. **Configurar fail2ban con reglas agresivas.** Bloqueo automático tras 5 intentos fallidos en 2 minutos. Tiempo de bloqueo mínimo: 24 horas para ataques de fuerza bruta.
5. **Política de contraseñas robusta.** Mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos. Rotación obligatoria cada 90 días. Uso de gestor de contraseñas corporativo.
6. **Revisar y auditar todas las cuentas de servicio.** Deshabilitar cuentas que no estén en uso activo. Implementar principio de mínimo privilegio. Auditoría trimestral de accesos.

Métricas Finales del Incidente

4 min	15 min	2h 35m	$0
TIEMPO DE DETECCIÓN (MTTD)	TIEMPO DE RESPUESTA (MTTR INICIAL)	TIEMPO RESOLUCIÓN TOTAL	IMPACTO EN DATOS / NEGOCIO

i Valor del SOC en este Incidente

Sin el monitoreo continuo del SOC ZAYWARE, este ataque habría pasado desapercibido durante horas o días. El atacante tenía acceso root y habría podido cifrar datos (ransomware), instalar backdoors o exfiltrar información confidencial. El costo estimado de un incidente no contenido en este escenario supera los **$250,000 MXN** en pérdida de datos, tiempo de respuesta no especializada y daño reputacional.

Analista: SOC ZAYWARE
Revisado por: Coordinador de Seguridad
Fecha de cierre: 14 de marzo de 2026

Próxima revisión: 21 de marzo de 2026
Seguimiento: Verificar implementación de recomendaciones
Estado: RESUELTO