Nota Técnica SAGE 001/2026

Vulnerabilidade CVE-2026-31431 — Kernel Linux (“Copy Fail”)

Versão 2 - 04 de maio de 2026

1. Contexto da Vulnerabilidade e Mitigação

O CEPEL informa que está monitorando atentamente a vulnerabilidade cibernética, divulgada recentemente pela comunidade global de segurança, que identificou uma falha relevante de escalonamento de privilégio, conhecida como “Copy Fail” (CVE-2026-31431), que afeta o subsistema criptográfico do kernel Linux (módulo *algif_aead*).

A falha em questão permite que um usuário com acesso local ao SAGE tente obter privilégio de administrador (“Root”).

Para o ambiente SAGE, os riscos são mitigados seguindo as instruções dos itens 3 e 4 e já validadas pela equipe de tecnologia do CEPEL.

> **Requisito para exploração:** o intruso precisa já estar autenticado no servidor-alvo, tendo superado todos os controles de acesso anteriores: firewall, VPN e credenciais de usuário. A vulnerabilidade não permite acesso remoto por si só.

2. Sistemas Afetados

Esta vulnerabilidade afeta a API de criptografia do Kernel Linux em diversas distribuições modernas (como Ubuntu, RHEL, Rocky, Debian), lançadas entre 2017 e 2026.

A vulnerabilidade está presente em kernels Linux versão **4.14 ou superior**. Kernels anteriores não contêm o commit vulnerável.

Sistema Operacional	Afetado?
RHEL 7.x / CentOS 7.x (kernel 3.10.x)	**NÃO — anterior ao kernel 4.14**
RHEL 8.x (kernel 4.18.x)	**POTENCIALMENTE**
RHEL 9.x (kernel 5.14.x)	**POTENCIALMENTE**
Rocky Linux 8.x (kernel 4.18.x)	**POTENCIALMENTE**
Rocky Linux 9.x (kernel 5.14.x)	**POTENCIALMENTE**

SAGE — Avaliação de Impacto

> O **SAGE** pode operar sobre RHEL/CentOS 7, 8 e 9. Portanto:
>
> - Instalações sobre **RHEL 7 / CentOS 7**: **não são afetadas.** O kernel 3.10.x é anterior ao commit vulnerável.
> - Instalações sobre **RHEL 8, RHEL 9 ou Rocky Linux**: **podem estar afetadas** e devem ser verificadas conforme a Seção 3.

3. Como Verificar se o Servidor Está Vulnerável

Execute os comandos abaixo a partir de qualquer conta de usuário. Não é necessário acesso root para verificar.

Passo 1 — Verificar a versão do kernel em execução

```
uname -r
```

Exemplos de resultado: `3.10.0-1160.el7` *(não afetado)* | `4.18.0-553.el8` *(verificar)*

Se o kernel for **anterior ao 4.14**: o sistema não é afetado. Se for **4.14 ou superior**: prossiga para os assos 2 (opcional) e 3.

Passo 2 — Verificar o estado do módulo em execução (opcional)

Para verificar se o subsistema que contém a vulnerabilidade chegou a ser ativado, execute o seguinte comando:

```
ls /sys/module/algif_aead && echo SUBSISTEMA ATIVO || echo subsistema inativo
```

Se retornar SUBSISTEMA ATIVO: o subsistema foi inicializado e a máquina está exposta.

Se retornar **subsistema inativo**: o subsistema que contém a vulnerabilidade não está ativo. **Atenção**: o fato de o subsistema não estar ativo não significa que a máquina esteja protegida, uma vez que essa ativação poderá ocorrer de forma automática quando da execução de algum processo que faça uso de suas funcionalidades.

Execute o Passo 3 para confirmar se há mitigação de boot ativa.

Passo 3 — Verificar se a mitigação de boot está ativa

```
grep -o initcall_blacklist=algif_aead_init /proc/cmdline && echo PROTEGIDO || echo
sem mitigacao
```

Se retornar **PROTEGIDO**: o workaround está ativo desde o último boot. Nenhuma ação adicional é necessária até que o patch definitivo seja publicado.

Se retornar **sem mitigacao**: aplique o workaround da Seção 4.

4. Procedimento de Mitigação

> **ATENÇÃO:** A fim de minimizar o impacto da aplicação da mitigação e evitar a parada total do SAGE, recomendamos que se execute as instruções no Servidor SAGE secundário, mantendo o servidor do SAGE Primário em operação. Após concluir e validar a mitigação no servidor SAGE secundário, repita as instruções no Servidor SAGE Primário.

> **Antes de iniciar:** os Passos 1 e 2 não interrompem o SAGE e podem ser executados com o sistema em produção. Já **o Passo 3** (reboot) requer a programação de uma janela de manutenção antes de sua execução.

Passo 1 — Inserir o parâmetro de mitigação via grubby

```
grubby --update-kernel=ALL --args="initcall_blacklist=algif_aead_init"
```

⚠ Requer execução como **root**

Passo 2 — Verificar que o parâmetro foi registrado em todos os kernels

```
grubby --info=ALL | grep args
```

O parâmetro initcall_blacklist=algif_aead_init deve aparecer na linha args de cada entrada.

Passo 3 — Reinicializar o servidor

```
reboot
```

⚠ Requer execução como **root**

Passo 4 — Confirmar a mitigação após o reboot

Após a reinicialização, execute novamente o Passo 3 da verificação (Seção 3):

```
grep -o initcall_blacklist=algif_aead_init /proc/cmdline && echo PROTEGIDO || echo VERIFICAR
```

Resultado esperado: PROTEGIDO

Se retornar **VERIFICAR**: o parâmetro não está ativo. Repita os Passos 1 e 2 e reinicialize novamente.

5. Impacto Operacional Resumido

Procedimento	Impacto no SAGE
Verificação — Seção 3 (todos os passos)	**Nenhum**
grubby — Passos 1 e 2 da mitigação	**Nenhum**
Reboot — Passo 3 da mitigação	**Indisponível durante a reinicialização**
Após reboot	**Operação normal restabelecida**

6. Validação Realizada pelo CEPEL

> O CEPEL executou os procedimentos acima em ambiente de laboratório e confirmou a **eficácia do workaround** contra o exploit publicado (“Copy Fail”). Após a aplicação do parâmetro via *grubby* e reboot, o exploit não foi capaz de obter privilégios de root no sistema testado.

7. Patch Definitivo e Próximos Passos

Até o presente momento, a Red Hat ainda não havia publicado o RHSA com a atualização de kernel definitiva para RHEL 8/9. O workaround via *grubby* é a medida de proteção disponível no momento e foi validada pelo CEPEL.

Assim que as novas versões oficiais de kernel forem publicadas pelos fabricantes, o CEPEL irá testá-las e publicará novas orientações com o procedimento a ser seguido para suas respectivas instalações.

- **Acompanhamento:** https://access.redhat.com/security/cve/cve-2026-31431
- **Suporte:** a equipe CEPEL está à disposição para apoio na aplicação do workaround em ambientes de produção.

Para qualquer consulta, dúvida ou assistência, por favor contactar os canais de suporte do SAGE ou através do e-mail: **sage@cepel.br**