

ソフトウェアエンジニアリング - サポート #301

Linuxカーネル脆弱性 CVE-2026-98432対応

2026/11/01 01:20 - 高橋 徹

ステータス:	進行中	開始日:	2026/11/01
優先度:	高め	期日:	
担当者:	高橋 徹	進捗率:	50%
カテゴリ:		予定工数:	0.00時間
対象バージョン:			
説明			
CVE-2026-98432 CVSS:9.8 (Critical)			
脅威：遠隔からroot権限で任意のコマンドを実行			
内容：IPv4のTCP処理でIPオプション付SYNパケットの再送／マルチパスTCPの競合処理等で use-after-free			
バグのためIPオプション解放済みメモリを別CPUが参照する競合状態が発生し、カーネルメモリの境界外読み出しとroot権限での任意コード実行に至る			
緩和策：IPオプション付パケットをFirewallでブロックする。MCTCPを無効化する。			
対象OS：Linuxカーネル4.4以降で本件修正前			
追加情報：			
• IPv4のIPオプション Record Route または Timestamp 付SYN			
参考情報：			
https://dnobori.cyber.ipa.go.jp/ppt/download/20261031/261031-HowToProtect-Linux-Kernel-CVE-2026-98432.pdf			

履歴

#1 - 2026/11/01 01:31 - 高橋 徹

MPTCPの有効／無効確認

```
$ sysctl net.mptcp.enabled
net.mptcp.enabled = 0
```

0 ならば無効、1 ならば有効

#2 - 2026/11/01 01:47 - 高橋 徹

IPオプション付SYNパケットの拒否設定

- nftablesの確認
nft --version
- firewallサービス稼働確認
systemctl status firewall
- nftablesテーブルを作成しルール適用（テンポラリ：firewall再起動で設定が失われる）

```
$ sudo nft add table inet cve_2026_98432
$ sudo nft add chain inet cve_2026_98432 prerouting \
> '{ type filter hook prerouting priority -310; policy accept; }'
$ sudo nft add rule inet cve_2026_98432 prerouting \
> ip protocol tcp ip hdrlength gt 5 counter drop
$
```

- nftables確認

```
$ sudo nft list table inet cve_2026_98432
table inet cve_2026_98432 {
    chain prerouting {
        type filter hook prerouting priority raw - 10; policy accept;
        ip protocol tcp ip hdrlength > 5 counter packets 0 bytes 0 drop
    }
}
```

#3 - 2026/11/01 01:48 - 高橋 徹

- ステータスを新規から進行中に変更

- 進捗率を0から50に変更