Cente Technical Information

発行番号	101-0123	Rev	第1版	発行日	2024/06/03
題名	メタデータ保護機能の管理用バッファがオーバフローしてしまう問題について				
情報分類	障害情報				
適用製品	・Cente FileSystem Ver6.10 ～ Ver6.50				
影響API	chg_filelen, rmdir, fopen, remove, rmdir_all, fwrite, rmdir_uni, fopen_uni ※ fopen, fopen_uniは"w"モード且つ既存ファイルを指定した場合に問題が生じます。				
関連資料	なし				

【現象】
FS_FAT_BLK_NUMを4で割り切れない値を設定した場合で且つ、複数のFATセクタにクラスタチェーンが跨がるようなファイル/ディレクトリにアクセスした場合にバッファのオーバーフローが発生する可能性があります。(CT_DISK_FULLエラーが発生する可能性があります)

《発生条件について》
以下の条件を満たした場合に発生します。
①FS_FAT_BLK_NUMを4で割り切れない値を設定した場合。
②jfsectnoで確保している要素以上にFATチェーンの作成/消去を行った場合。
　※ フラグメンテーションが発生して複数のFATセクタにクラスタチェーンが跨ると、要素以上になる可能性があります。
③影響APIを実行した場合。

【原因】
メタデータ保護機能のバックアップを行う際、FAT1の情報をFAT2にコピーをします。
コピーを行う際、以下の情報を使用します。
・J_FSECT_SZ　バックアップ対象のセクタの最大数を管理
・jfsectno　バックアップ対象のセクタを記憶する配列テーブル
コピーを行う際、バックアップの範囲は最大J_FSECT_SZのセクタ数までバックアップを行いますが、
設定値によってjfsectnoの要素数がJ_FSECT_SZよりも小さくなる場合がありました。
その結果、バッファのオーバーフローが発生してしまう可能性があります。

以下、J_FSECT_SZ及びjfsectnoの計算式になります。
■fs_journal.c
```
static ct_uint32_t jfsectno[FS_JNL_DV_MAX][SECT_SZ / sizeof(ct_uint32_t) * J_FSECT_SCT];
```

■fs_journal.h
#define J_FSECT_SZ　(FS_DATA_SZ / FS_AUS_SZ * FS_FAT_BLK_NUM)
#define J_FSECT_SCT　(J_FSECT_SZ * 4 / SECT_SZ)

■fs_cfg.h
#define FS_DATA_SZ　131072
#define FS_AUS_SZ　4096
#define FS_FAT_BLK_NUM 5
#define FS_DIR_BLK_NUM 8
#define SECT_SZ　512

	異常	正常	
J_FSECT_SZのサイズ	160	160	→ OK
J_FSECT_SCTのサイズ	1	2	→ NG
jfsectnoの要素数	128	256	

本来、jfsectnoはJ_FSECT_SZよりも大きい配列の要素を確保する必要がありますが、
J_FSECT_SCTのサイズが小数点を考慮できておりませんでした。
その結果、jfsectnoよりもJ_FSECT_SZが大きくなってしまい、現象の発生条件を満たすことによりオーバーフローしてしまう場合がありました。

【回避方法】
■運用での回避方法
ありません。

■プログラムによる回避方法
修正ソースにつきましては、弊社サポートまでお問い合わせ下さい。

以上