

Cente Technical Information

発行番号	101-0106	Rev	第1版	発行日	2019/11/01
題名	rmdir_all_uni、dinfo_uni、readdir_wc_uni実行時に内部構造体のメモリ破壊が発生する不具合について				
情報分類	障害情報				
適用製品	・Cente FileSystem Ver6.30 ~ Ver6.41				
影響API	rmdir_all_uni, dinfo_uni, readdir_wc_uni				
関連資料	なし				

【現象】

【影響API】の引数に対して、以下の条件を満たした場合に構造体の情報が壊れ、期待した検索結果が取得できない現象が発生します。

《発生条件》

- ・rmdir_all_uni() : 引数"dname"に130文字以上のフルパスを渡した場合。
- ・dinfo_uni() : 引数"dname"に130文字以上のフルパスを渡した場合。
- ・readdir_wc_uni(): 引数"targetname"に130文字以上の検索文字列(ファイル名)を渡した場合。

【原因】

【影響API】では引数として渡されたUNICODE文字列をfs_strncpy_uni()を使用し、内部の構造体資源にコピーしておりますが、関数の引数に渡している値に誤りがありました。

fs_strncpy_uni()ではコピーするUNICODE文字列のサイズとして「文字数」を指定する仕様になっておりますが、「バイト数」を指定していたため、正常時の倍の文字数をコピーしていました。(1文字 = 2バイト)
その結果、コピー先アドレスの範囲を超えたコピーが行われてしまい、メモリ破壊が発生していました。

【回避方法】

■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