CVE-2015-8026

描述：Heap-based buffer overflow in the verify\_vbr\_checksum function in exfatfsck in exfat-utils before 1.2.1 allows remote attackers to cause a denial of service (infinite loop) or possibly execute arbitrary code via a crafted filesystem.

软件：exfat-utils

源码：libexfat/mount.c

出现位置：209-251行

关键源码：

ef->zero\_cluster = malloc(CLUSTER\_SIZE(\*ef->sb));

if (ef->zero\_cluster == NULL)

{

exfat\_close(ef->dev);

free(ef->sb);

exfat\_error("failed to allocate zero sector");

return -ENOMEM;

}

/\* use zero\_cluster as a temporary buffer for VBR checksum verification \*/

if (!verify\_vbr\_checksum(ef->dev, ef->zero\_cluster, SECTOR\_SIZE(\*ef->sb)))

{

free(ef->zero\_cluster);

exfat\_close(ef->dev);

free(ef->sb);

return -EIO;

}

memset(ef->zero\_cluster, 0, CLUSTER\_SIZE(\*ef->sb));

if (ef->sb->version.major != 1 || ef->sb->version.minor != 0)

{

free(ef->zero\_cluster);

exfat\_close(ef->dev);

exfat\_error("unsupported exFAT version: %hhu.%hhu",

ef->sb->version.major, ef->sb->version.minor);

free(ef->sb);

return -EIO;

}

if (ef->sb->fat\_count != 1)

{

free(ef->zero\_cluster);

exfat\_close(ef->dev);

exfat\_error("unsupported FAT count: %hhu", ef->sb->fat\_count);

free(ef->sb);

return -EIO;

}

/\* officially exFAT supports cluster size up to 32 MB \*/

if ((int) ef->sb->sector\_bits + (int) ef->sb->spc\_bits > 25)

{

free(ef->zero\_cluster);

exfat\_close(ef->dev);

exfat\_error("too big cluster size: 2^%d",

(int) ef->sb->sector\_bits + (int) ef->sb->spc\_bits);

free(ef->sb);

return -EIO;