Hash Suite - Windows password security audit tool. GUI, reports in PDF.

[<prev] [next>] [<thread-prev] [day] [month] [year] [list]

```
Date: Mon, 28 Dec 2020 16:14:59 +0800
From: butt3rflyh4ck <butterflyhuangxx@...il.com>
To: oss-security@...ts.openwall.com
Subject: Re: CVE-2020-27815 Linux kernel: jfs:
 array-index-out-of-bounds in dbAdjTree
```

Patch for this issue :

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c61b3e4839007668360ed8b87d7da96d2e59fc6c

```
Regards.
 butt3rflyh4ck.
```

```
On Tue, Dec 1, 2020 at 1:50 AM butt3rflyh4ck <butterflyhuangxx@...il.com>
wrote:

> Hello,
>
> I report an array-index-out-of-bounds bugs in fs/jfs/jfs_dmap.c in
> dbAdjTree and reproduce it in Linux kernel 5.9.6 version.
>
> Description:
>
> In the Linux kernel through 5.9.6, there is a
> array-index-out-of-bounds in fs/jfs/jfs_dmap.c in dbAdjTree and it may
> cause out of bounds read and Denial of Service.
>
> Root Cause:
>
> the dmtree_t is that
>  typedef union dmtree {
>  struct dmaptree t1;
>  struct dmapctl t2;
> } dmtree_t;
>
>  the dmaptree is that
>   struct dmaptree {
>    __le32 nleafs; /* 4: number of tree leafs */
>    __le32 l2nleafs; /* 4: l2 number of tree leafs */
>    __le32 leafidx; /* 4: index of first tree leaf */
>    __le32 height; /* 4: height of the tree */
>   s8 budmin; /* 1: min l2 tree leaf value to combine */
>   s8 stree[TREESIZE]; /* TREESIZE: tree */
>   u8 pad[2]; /* 2: pad to word boundary */
>   };the TREESIZE is totally 341.
>
> the dmapctl is that:
> struct dmapctl {
> __le32 nleafs; /* 4: number of tree leafs */
> __le32 l2nleafs; /* 4: l2 number of tree leafs */
> __le32 leafidx; /* 4: index of the first tree leaf */
> __le32 height; /* 4: height of tree */
> s8 budmin; /* 1: minimum l2 tree leaf value */
> s8 stree[CTLTREESIZE]; /* CTLTREESIZE: dmapctl tree */
> u8 pad[2714]; /* 2714: pad to 4096 */
> }; /* - 4096 - */
> the CTLTREESIZE is totally 1365.
> The dmt_stree was used in dbAdjTree. Since dmt_stree can refer to the
> stree in both structures dmaptree and dmapctl. the stree size is not
> consistent, may it cause index out of range.
>
> CVE assigned :
> CVE-2020-27815
>
> Patch:
> It's in linux-next now, not available in upstream.
>
> Credit:
> This issue was discovered by the ADLab of venustech.
>
> Regards.
>  butt3rflyh4ck.
>
```

Powered by blists - more mailing lists

Please check out the Open Source Software Security Wiki, which is counterpart to this mailing list.

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.