OpenPrinting / **cups** Public

Code Issues 22 Pull requests 7 Discussions Actions Projects

Commit b7c2525

michaelrsweet committed 2 weeks ago · 5 / 5 · Verified

```
Limit num_bytes for SNMP string values.
```

2.4.x · v2.4.18 v2.4.17

1 parent c05d32b commit b7c2525

2 files changed +9 -5

Top

Filter files...

- cups
  - snmp-private.h
  - snmp.c

Search within code

cups/snmp-private.h

```
@@ -1,7 +1,7 @@
 /*
  * Private SNMP definitions for CUPS.
  *
-  * Copyright © 2020-2024 by OpenPrinting.
+  * Copyright © 2020-2026 by OpenPrinting.
  * Copyright © 2007-2014 by Apple Inc.
  * Copyright © 2006-2007 by Easy Software Products, all rights reserved.
  *
@@ -58,9 +58,9 @@ typedef enum cups_asn1_e cups_asn1_t; /**** ASN1
 request/object types ****/
```

```
58  58
59  59    typedef struct cups_snmp_string_s   /**** String value ****/
60  60    {
61      -   unsigned char bytes[CUPS_SNMP_MAX_STRING];
62      -                   /* Bytes in string */
63  61      unsigned  num_bytes;      /* Number of bytes */
    62  +   unsigned char bytes[CUPS_SNMP_MAX_STRING + 1];
    63  +                   /* Bytes in string */
64  64    } cups_snmp_string_t;
65  65
66  66    union cups_snmp_value_u         /**** Object value ****/
```

cups/snmp.c

```
    ...   @@ -1,7 +1,7 @@
1   1     /*
2   2      * SNMP functions for CUPS.
3   3      *
4       - * Copyright © 2020-2024 by OpenPrinting.
    4   + * Copyright © 2020-2026 by OpenPrinting.
5   5     * Copyright © 2007-2019 by Apple Inc.
6   6     * Copyright © 2006-2007 by Easy Software Products, all rights reserved.
7   7     *
          @@ -1042,10 +1042,14 @@ asn1_decode_snmp(unsigned char *buffer, /* I -
          Buffer */
1042  1042              case CUPS_ASN1_OCTET_STRING :
1043  1043              case CUPS_ASN1_BIT_STRING :
1044  1044              case CUPS_ASN1_HEX_STRING :
1045      -               packet->object_value.string.num_bytes = length;
1046  1045              asn1_get_string(&bufptr, bufend, length,
1047  1046                              (char *)packet->object_value.string.bytes,
1048  1047                              sizeof(packet->object_value.string.bytes));
    1048  +
    1049  +               if (length >= sizeof(packet->object_value.string.bytes))
    1050  +                 packet->object_value.string.num_bytes = sizeof(packet-
          >object_value.string.bytes) - 1;
    1051  +               else
    1052  +                 packet->object_value.string.num_bytes = length;
1049  1053              break;
1050  1054
```

```
1051  1055            case CUPS_ASN1_OID :
```

Comments 0

Please sign in to comment.