OpenPrinting / **cups** Public

Code | Issues 22 | Pull requests 7 | Discussions | Actions | Projects

Commit `d7fe0f5`

michaelrsweet committed 2 weeks ago · 5 / 5 · Verified

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

master

1 parent 4ac17a8 commit d7fe0f5

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.
 //
@@ -55,9 +55,9 @@ typedef enum cups_asn1_e cups_asn1_t; // ASN1
 request/object types
```

```
55  55
56  56    typedef struct cups_snmp_string_s   // String value
57  57    {
58      -   unsigned char bytes[CUPS_SNMP_MAX_STRING];
59      -                   // Bytes in string
60  58      unsigned  num_bytes;      // Number of bytes
    59  +   unsigned char bytes[CUPS_SNMP_MAX_STRING + 1];
    60  +                   // Bytes in string
61  61    } cups_snmp_string_t;
62  62
63  63    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      *
       @@ -1014,10 +1014,14 @@ asn1_decode_snmp(unsigned char *buffer, /* I -
       Buffer */
1014 1014              case CUPS_ASN1_OCTET_STRING :
1015 1015              case CUPS_ASN1_BIT_STRING :
1016 1016              case CUPS_ASN1_HEX_STRING :
1017     -              packet->object_value.string.num_bytes = length;
1018 1017              asn1_get_string(&bufptr, bufend, length,
1019 1018                              (char *)packet->object_value.string.bytes,
1020 1019                              sizeof(packet->object_value.string.bytes));
     1020 +
     1021 +              if (length >= sizeof(packet->object_value.string.bytes))
     1022 +                packet->object_value.string.num_bytes = sizeof(packet-
       >object_value.string.bytes) - 1;
     1023 +              else
     1024 +                packet->object_value.string.num_bytes = length;
1021 1025                break;
1022 1026
```

```
1023  1027            case CUPS_ASN1_OID :
```

Comments 0

Please sign in to comment.