

OpenPrinting / cups Public

<> Code Issues 19 Pull requests 8 Discussions Actions Projects

Commit 88516bf

michaelrsweet committed 2 weeks ago · ✖ 4/5 · Verified

CVE-2026-27447: The scheduler treated local user and group names as case-insensitive.

master

1 parent [4bcd4b4](#) commit 88516bf

1 file changed +16 -17 lines changed

Top

▼ scheduler

auth.c

1 file changed +16 -17 lines changed

▼ scheduler/auth.c

```

@@ -1,7 +1,7 @@
1 1 /*
2 2  * Authorization routines for the CUPS scheduler.
3 3  *
4 - * Copyright © 2020-2025 by OpenPrinting.
4 + * Copyright © 2020-2026 by OpenPrinting.
5 5  * Copyright © 2007-2019 by Apple Inc.
6 6  * Copyright © 1997-2007 by Easy Software Products, all rights reserved.
7 7  *

@@ -1239,7 +1239,7 @@ cupsdCheckGroup(
1239 1239     group = getgrnam(groupname);
1240 1240     endgrent();

```

```

1241 1241
1242 -   if (group != NULL)
1242 +   if (user && group)
1243 1243     {
1244 1244     /*
1245 1245     * Group exists, check it...
@@ -1253,7 +1253,7 @@ cupsdCheckGroup(
1253 1253     * User appears in the group membership...
1254 1254     */
1255 1255
1256 -   if (!_cups_strerror(username, group->gr_mem[i]))
1256 +   if (!strcmp(user->pw_name, group->gr_mem[i]))
1257 1257     return (1);
1258 1258     }
1259 1259
@@ -1264,25 +1264,24 @@ cupsdCheckGroup(
1264 1264     * belongs to...
1265 1265     */
1266 1266
1267 -   if (user)
1268 -   {
1269 -       int    ngroups;        /* Number of groups */
1267 +   int    ngroups;        /* Number of groups */
1270 1268     # ifdef __APPLE__
1271 -       int    groups[2048];   /* Groups that user belongs to */
1269 +       int    groups[2048];   /* Groups that user belongs to */
1272 1270     # else
1273 -       gid_t  groups[2048];   /* Groups that user belongs to */
1271 +       gid_t  groups[2048];   /* Groups that user belongs to */
1274 1272     # endif /* __APPLE__ */
1275 1273
1276 -       ngroups = (int)(sizeof(groups) / sizeof(groups[0]));
1274 +       ngroups = (int)(sizeof(groups) / sizeof(groups[0]));
1277 1275     # ifdef __APPLE__
1278 -       getgrouplist(username, (int)user->pw_gid, groups, &ngroups);
1276 +       getgrouplist(user->pw_name, (int)user->pw_gid, groups, &ngroups);
1279 1277     # else
1280 -       getgrouplist(username, user->pw_gid, groups, &ngroups);
1278 +       getgrouplist(user->pw_name, user->pw_gid, groups, &ngroups);
1281 1279     #endif /* __APPLE__ */

```

1282	1280	
1283		- for (i = 0; i < ngroups; i ++)
1284		- if ((int)groupid == (int)groups[i])
1285		- return (1);
1281		+ for (i = 0; i < ngroups; i ++)
1282		+ {
1283		+ if ((int)groupid == (int)groups[i])
1284		+ return (1);
1286	1285	}
1287	1286	#endif /* HAVE_GETGROUPLIST */
1288	1287	}
		@@ -2005,8 +2004,8 @@ cupsdIsAuthorized(cupsd_client_t *con, /* I - Connection */
2005	2004	name;
2006	2005	name = (char *)cupsArrayNext(best->names))
2007	2006	{
2008		- if (!_cups_strcasecmp(name, "@OWNER") && owner &&
2009		- !_cups_strcasecmp(username, ownername))
2007		+ if (!_cups_strcasecmp(name, "@OWNER") && owner && pw &&
2008		+ !strcmp(pw->pw_name, ownername))
2010	2009	return (HTTP_STATUS_OK);
2011	2010	else if (!_cups_strcasecmp(name, "@SYSTEM"))
2012	2011	{
		@@ -2018,7 +2017,7 @@ cupsdIsAuthorized(cupsd_client_t *con, /* I - Connection */
2018	2017	if (cupsdCheckGroup(username, pw, name + 1))
2019	2018	return (HTTP_STATUS_OK);
2020	2019	}
2021		- else if (!_cups_strcasecmp(username, name))
2020		+ else if (pw && !strcmp(pw->pw_name, name))
2022	2021	return (HTTP_STATUS_OK);
2023	2022	}
2024	2023	

Comments 0



Please [sign in](#) to comment.