sysstat overflow on 32-bit systems

Moderate sysstat published **GHSA-q8r6-g56f-9w7x** 21 days ago

Package

sysstat (GitHub Actions)

Affected versions	Patched versions
>= 9.1.6	12.7.1

Description

Summary

On 32 bit systems, an arithmetic overflow present in allocate_structures can be triggered when displaying activity data files and may lead to a variety of exploit primitives due to an incorrectly sized buffer.

Details

Issue: size_t overflow in sa_common.c (GHSL-2022-074)

allocate_structures function located in sa_common.c insufficiently checks bounds before arithmetic multiplication ([1]) allowing for an overflow in the size allocated for the buffer representing system activities.

```
void allocate_structures(struct activity *act[])
{
        int i, j;

        for (i = 0; i < NR_ACT; i++) {
                if (act[i]->nr_ini > 0) {
                        for (j = 0; j < 3; j++) {
                                SREALLOC(act[i]->buf[j], void,
                                                (size_t) act[i]->msize * (size_t) act[i]-
>nr_ini * (size_t) act[i]->nr2);  // [1]
                        }
                        act[i]->nr_allocated = act[i]->nr_ini;
                }
        }
  }
```

Impact

This issue may lead to Remote Code Execution (RCE)

For more information

If you have any questions or comments about this advisory:

- Email me at sysstat [at] orange [dot] fr

Severity

Moderate

CVE ID

CVE-2022-39377

Weaknesses

No CWEs