New issue

Add STProcessMonitor Driver #268

Closed #279

wwwab123 opened on Feb 12 · edited by wwwab123 Edits

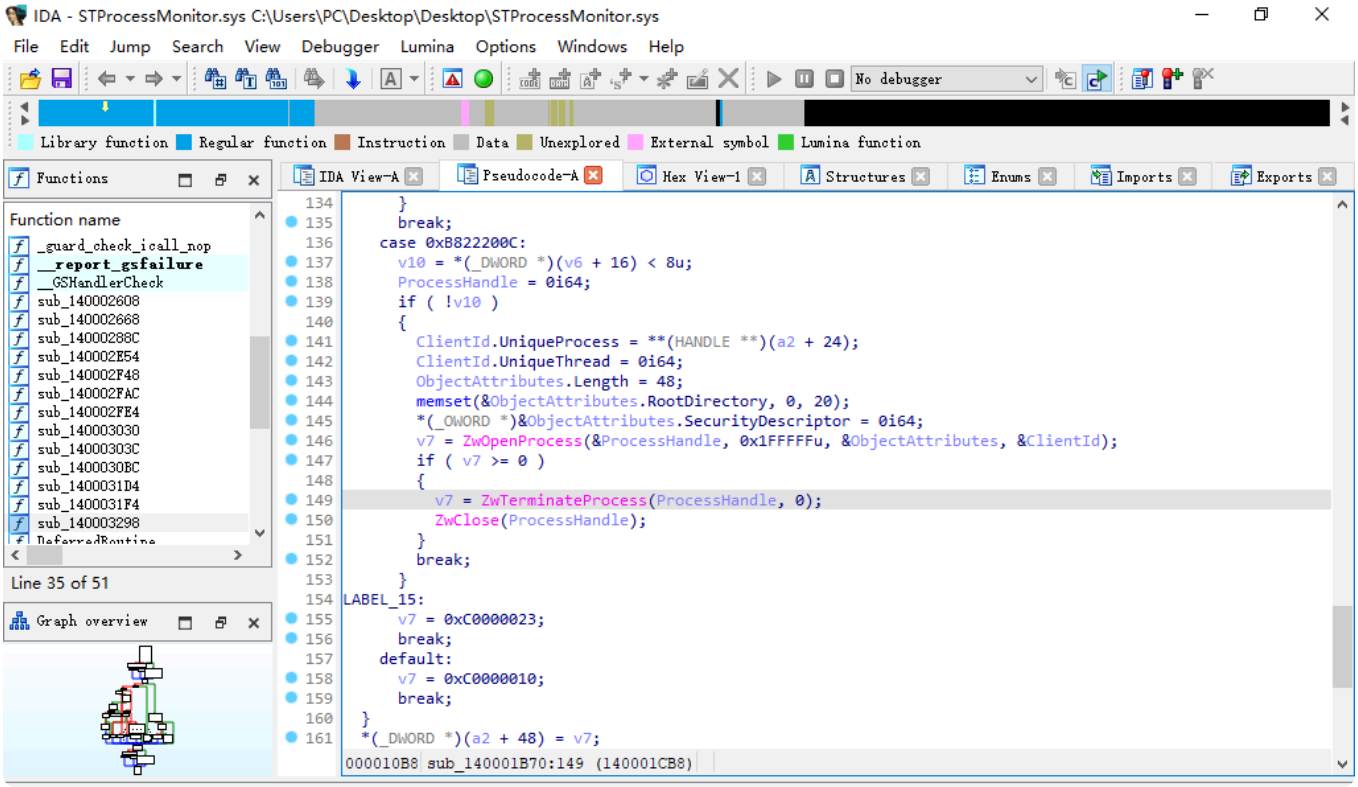
CVE-2025-70795 vulnerability in STProcessMonitor Driver from Safetica

- Affects:
  - **Legacy builds (11.11.4.0+)** -> low-privilege BYOVD abuse
  - **Current build (11.26.18.0+)** -> LocalSystem-privilege BYOVD abuse

Driver hashes:

- `STProcessMonitor.sys` **11.11.4.0** SHA256: `70bcec00c215fe52779700f74e9bd669ff836f594df92381cbfb7ee0568e7a8b`

STProcessMonitor.zip



Poc see: https://github.com/wwwab123/BYOVD/tree/main/STProcessMonitor114-Killer

- `STProcessMonitor.sys` **11.26.18.0** SHA256:
  `5b4f59236a9b950bcd5191b35d19125f60cfb9e1a1e1aa2e4f914b6745dde9df`

STProcessMonitor.zip

Poc (need LocalSystem-privilege) see:
https://github.com/wwwab123/BYOVD/tree/main/STProcessMonitor2618-Killer

👍 1 ❤️ 1

wwwab123 mentioned this on Feb 24

STProcessMonitor-Killer: CVE-2025-70795 BlackSnufkin/BYOVD#5

MHaggis added a commit that references this issue on Mar 21

`Add 4 new drivers, 3 sample updates, and 2 data quality fixes from is.` ···

`fb5f0ad`

MHaggis mentioned this on Mar 21

Add 4 new drivers, update 3 entries, fix 2 data quality issues (9 issues resolved) #279

MHaggis added a commit that references this issue 3 weeks ago

`Add 4 new drivers, 3 sample updates, and 2 data quality fixes from is.` ···

`eea8326`

MHaggis closed this as completed in eea8326 3 weeks ago

wwwab123 mentioned this 2 weeks ago

CVE-2025-70795 and CVE-2026-0828 oxfemale/KillChain#1

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Add 4 new drivers, update 3 entries, fix 2 data quality issues (9 issues resolved)
magicsword-io/LOLDrivers

Participants