New issue

Jump to bottom

CVE-2020-8446: analysisd: syscheck decoder location path injection. #1813

Open **cpu** opened this issue on Jan 15, 2020 · 1 comment

cpu commented on Jan 15, 2020 • edited Contributor

The `ossec-analysisd` 's syscheck decoder (`src/analysisd/decoders/syscheck.c`) performs unsafe path handling using the received agent name when trying to get the agent file. The `DB_File` function uses the agent name unsanitized when building a file name to be used with `fopen` .

ossec-hids/src/analysisd/decoders/syscheck.c
Lines 212 to 216 in abb36d4

```
212     /* Get agent file */
213     snprintf(sdb.buf, OS_FLSIZE , "%s/%s", SYSCHECK_DIR, agent);
214
215     /* r+ to read and write. Do not truncate */
216     sdb.agent_fps[i] = fopen(sdb.buf, "r+");
```

Processing a syscheck message like `8:a/../../etc/shared/test.txt:aaaaaaa aaaa'` from an agent named `test` sending from localhost results in an `open` for `queue/syscheck/(test) 127.0.0.1->a/../../etc/shared/test.txt`

This will fail with `ENOTDIR` because the part of the path the attacker can't control remotely (`(test) 127.0.0.1->a`) is not a directory. Creating it first by sending a message like `8:a:aaaaaaa aaaa` seems like a potential solution at first but won't work because while the file `queue/syscheck/(test) 127.0.0.1->a` will be created it won't be created as a *directory* but a regular file.

I suspect this means that the bug is only useful to local attackers (that can write directly to the ossec queue). Writing directly to the queue allows full control of the `lf->location` used as the `agent` argument to `fopen` and can cause the syscheck DB file to be created in an attacker controlled location within the `chroot` . Remote attackers can not control the full `lf->location` since the `ossec-remoted` ensures the prefix of agent name and source IP is always present.

Likely the best fix is to use the `w_ref_parent_folder` function from `src/shared/file_op.c` on the location field populated by `OS_CleanMSG` and rejecting any values that have a `1` return from that function.

cpu mentioned this issue on Jan 15, 2020

OSSEC-HIDS Security Audit Findings #1821

Closed

cpu changed the title ~~analysisd: syscheck decoder location path injection.~~ **CVE-2020-8446: analysisd: syscheck decoder location path injection.** on Jan 30, 2020

cpu commented on Jan 30, 2020 Contributor Author

This was assigned CVE-2020-8446

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant