CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-055

Critical Vulnerability in the Solaris PAM Library

November 5, 2020 — v1.0

TLP:WHITE

History:

- *5/11/2020 — v1.0 – Initial publication*

Summary

Within its monthly Critical Patch Update Advisory, Oracle released patch for a critical vulnerability affecting Solaris Pluggable Authentication Module (PAM) [1].

FireEye discovered during an investigation traces of exploitation of this vulnerability since 2018 [2]. Moreover, FireEye associated the vulnerability with *Oracle Solaris SSHD Remote Root Exploit* identified on black-market for sale. This vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris.

Technical Details

The vulnerability received CVE-2020-14871 [3] and has CVSS score 8.8. It occurs in the PAM library. PAM enables a Solaris application to authenticate users while allowing the system administrator to configure authentication parameters (e.g., password complexity and expiration) in one location that is consistently enforced by all applications. The actual vulnerability is a stack-based buffer overflow located in the PAM `parse_user_name` function. It is triggered when a username longer than `PAM_MAX_RESP_SIZE` (512 bytes) is passed to `parse_user_name`. The vulnerability has likely existed for decades.

SSH Keyboard-Interactive authentication is a *passthrough* authentication mechanism where the SSH protocol relays prompts and responses between the server's PAM libraries and the client. It was designed to support custom forms of authentication such as two-factor without modifying the SSH protocol. By manipulating SSH client settings to force Keyboard-Interactive authentication to prompt for the username rather than sending it through normal means, an attacker can also pass unlimited input to the PAM `parse_user_name` function.

A proof-of-concept exploit that can be used to see if a server is vulnerable is available in [4]. FireEye has also observed that if a `/core` file exists on a Solaris machine, and the `file` command reports that it is from `sshd`, these indicators are consistent with this vulnerability having been exploited [4].

Affected Products

The vulnerability exists in [4]:

- Solaris 9 (some releases)
- Solaris 10 (all releases)
- Solaris 11.0[1]
- Illumos (OpenIndiana 2020.04)

Recommendations

A patch from Oracle for Solaris 10 and 11 is described in the October 2020 Critical Patch Update [1].

Workarounds

As Solaris 9 is no longer supported, Oracle has not released a patch. For Solaris 9, as well as for Solaris 10 or 11 systems where patching is inconvenient, FireEye recommends editing the `/etc/ssh/sshd_config` file to add the lines:

```
ChallengeResponseAuthentication no
KbdInteractiveAuthentication no
```

and restart the SSH server. While this removes the opportunity to exploit the vulnerability using SSH Keyboard-Interactive authentication, there may be other ways to attack the `parse_user_name` function and it is recommended using this workaround only as a stopgap until Solaris 9 systems can be upgraded, or the October patch can be accessed and installed for supported Solaris versions [4].

References

[1] https://www.oracle.com/security-alerts/cpuoct2020.html

[2] https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-14871

[4] https://www.fireeye.com/blog/threat-research/2020/11/critical-buffer-overflow-vulnerability-in-solaris-can-allow-remote-takeover.html

[1] While the `parse_user_name` function remains vulnerable in unpatched Solaris 11.1 and later, unrelated changes to the PAM library truncate the username before the vulnerable function receives it, rendering the issue non-exploitable via SSH. If the `parse_user_name` function were reachable in another context, then the vulnerability could become exploitable.