CERT-EU

Security Advisory 2022-037

Path Traversal SPL Injection in Splunk Products

May 20, 2022 — v1.0

TLP:WHITE

History:

- *20/05/2022 — v1.0 – Initial publication*

Summary

On May 3rd, 2022, Splunk released a security advisory for path traversal in search parameter that can potentiall allow external content injection [1]. An attacker can cause the application to load data from incorrect endpoints, URLs leading to outcomes such as running arbitrary SPL queries [3].

A vulnerability was found in Splunk Enterprise up to 8.1.1 and it has been declared as **critical** and named **CVE-2022-26889** [1].

Technical Details

This vulnerability affects processing of the component Search Parameter Handler. The manipulation with an unknown input leads to a privilege escalation vulnerability. The exploitation appears to be easy. The attack can be initiated remotely. No authentication is required for a successful exploitation. Neither more technical details, nor an exploit is yet publicly available [2].

Affected products

Splunk Enterprise versions before 8.1.2. The vulnerability does not impact Splunk Cloud Platform instances [4].

Recommendations

CERT-EU strongly recommends to upgrade Splunk Enterprise to 8.1.2 or later.

Workarounds

The vulnerability impacts instances with Splunkweb enabled [1]. More information on disabling Splunkweb can be found in Securing Splunk Enterprise [5] and Splunk Enterprise administration manuals [6].

References

[1] https://www.splunk.com/en_us/product-security/announcements/svd-2022-0506.html

[2] https://vuldb.com/?id.199240

[3] https://research.splunk.com/application/path_traversal_spl_injection/

[4] https://nvd.nist.gov/vuln/detail/CVE-2022-26889

[5] https://docs.splunk.com/Documentation/Splunk/latest/Security/DisableunnecessarySplunkcomponents?_gl=1*dumf7s*_ga*NDYxOTU3ODcyLjE2NTMwNjAzNTE.*_gid*MTUyMjI1ODMzNi4xNjUzMDYwMzUy&_ga=2.98395231.1522258336.1653060352-461957872.1653060351

[6] https://docs.splunk.com/Documentation/Splunk/latest/Admin/Webconf?_gl=1*oiaygj*_ga*NDYxOTU3ODcyLjE2NTMwNjAzNTE.*_gid*MTUyMjI1ODMzNi4xNjUzMDYwMzUy&_ga=2.24651898.1522258336.1653060352-461957872.1653060351