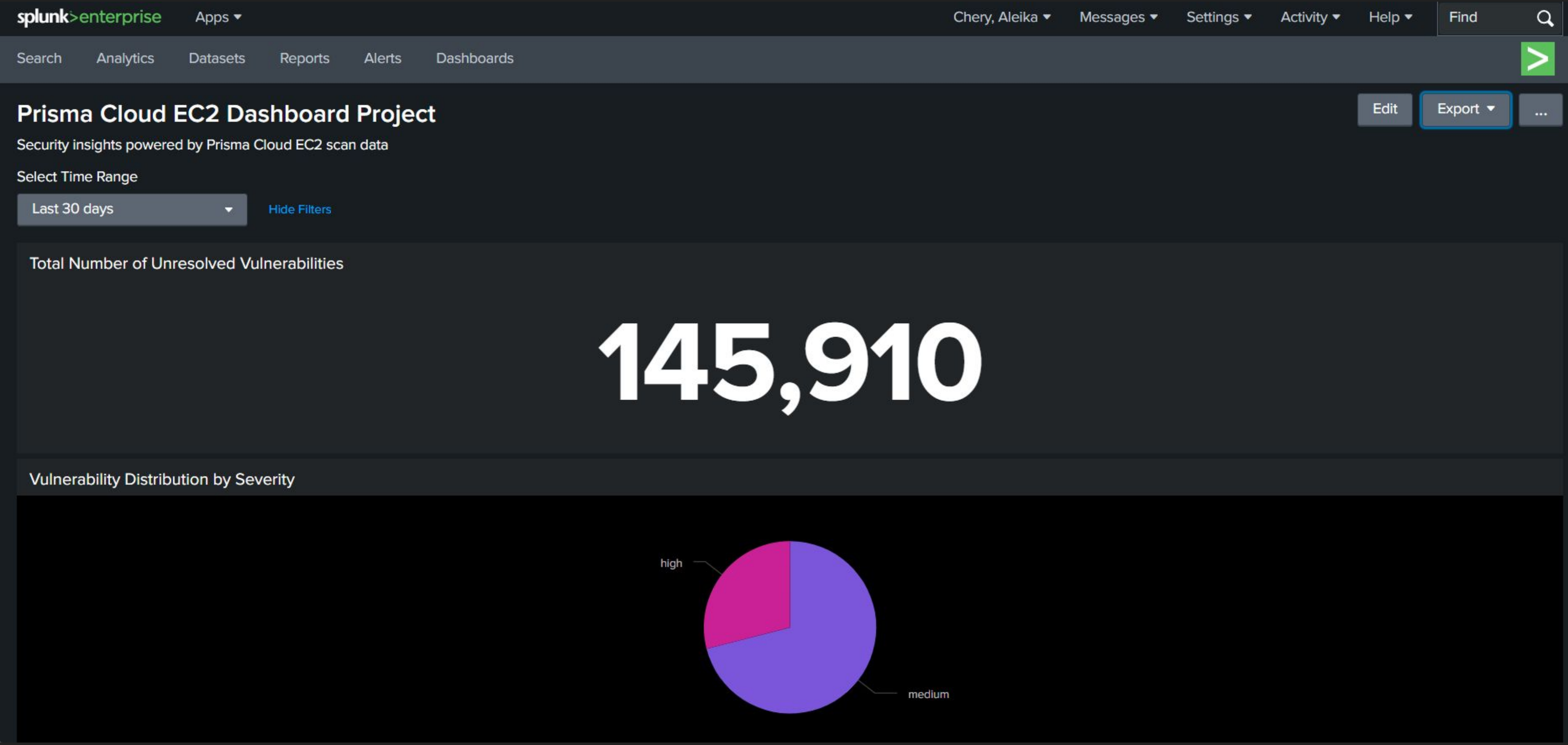
Splunk Dashboard: Prisma Cloud EC2 Vulnerabilities Scan

Aleika Chery
MSK DigITs Internship Summer 2025



Prisma Cloud EC2 Dashboard Project

Security insights powered by Prisma Cloud EC2 scan data

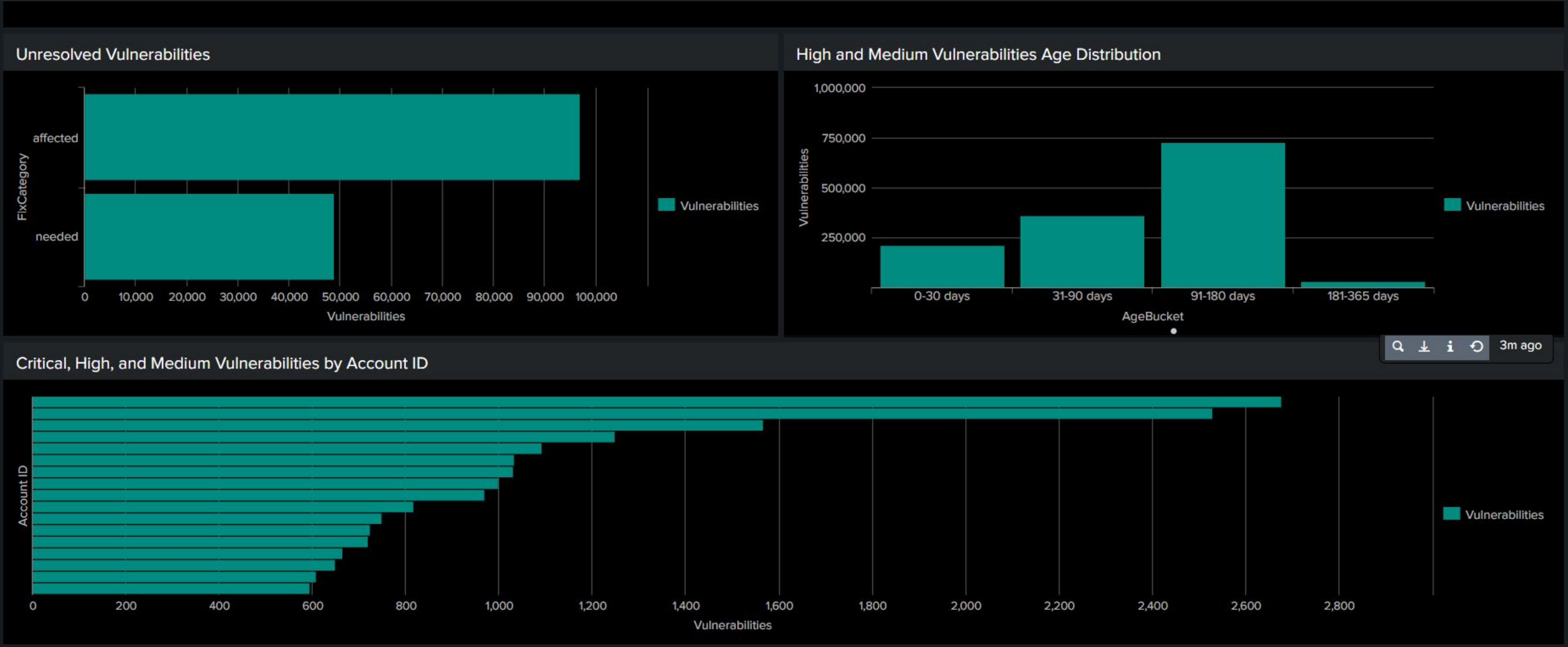
Select Time Range

Last 30 days ▾

Total Number of Unresolved Vulnerabilities

145,910

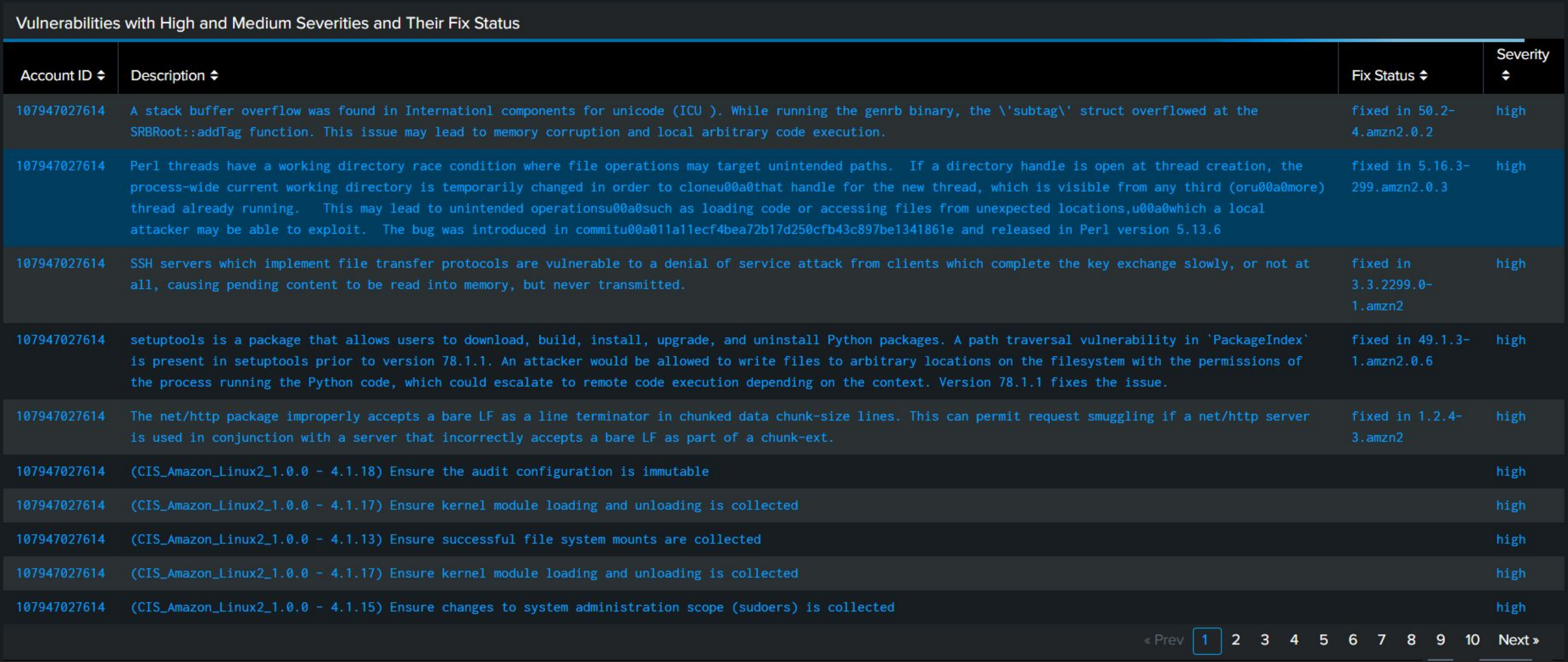
Vulnerability Distribution by Severity



Unresolved Vulnerabilities

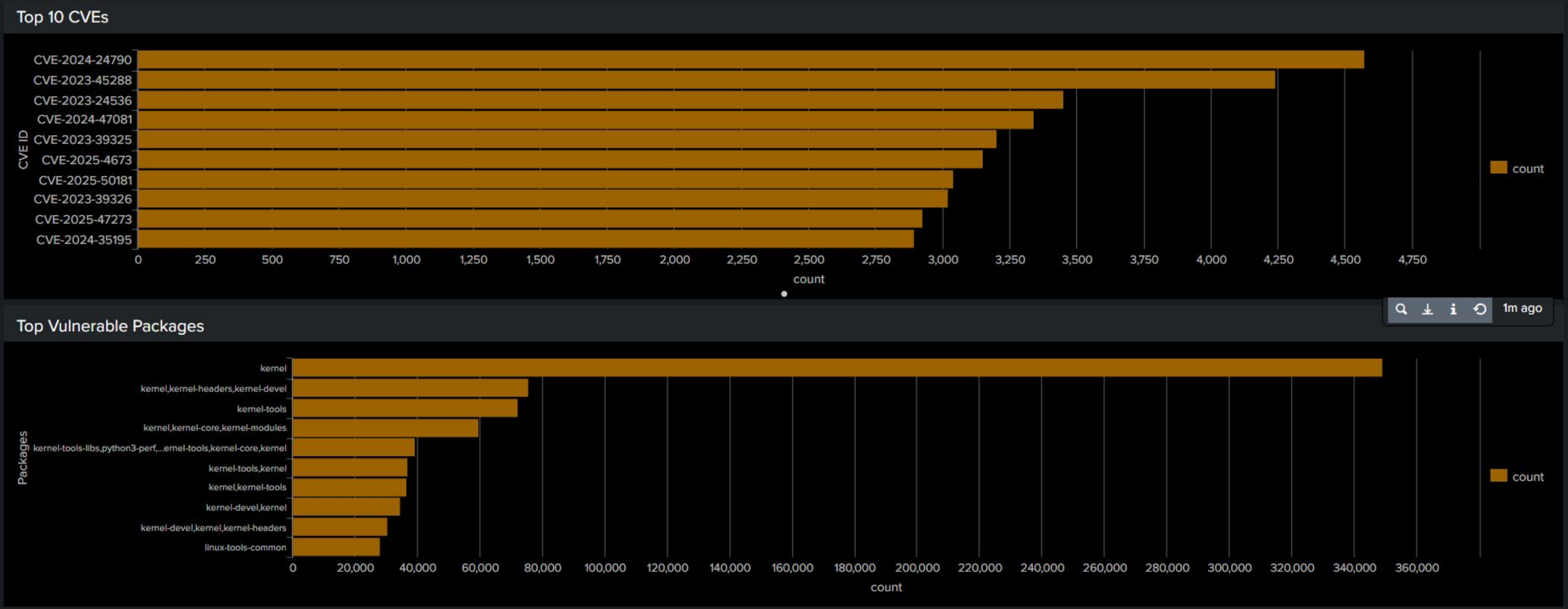
High and Medium Vulnerabilities Age Distribution

Critical, High, and Medium Vulnerabilities by Account ID



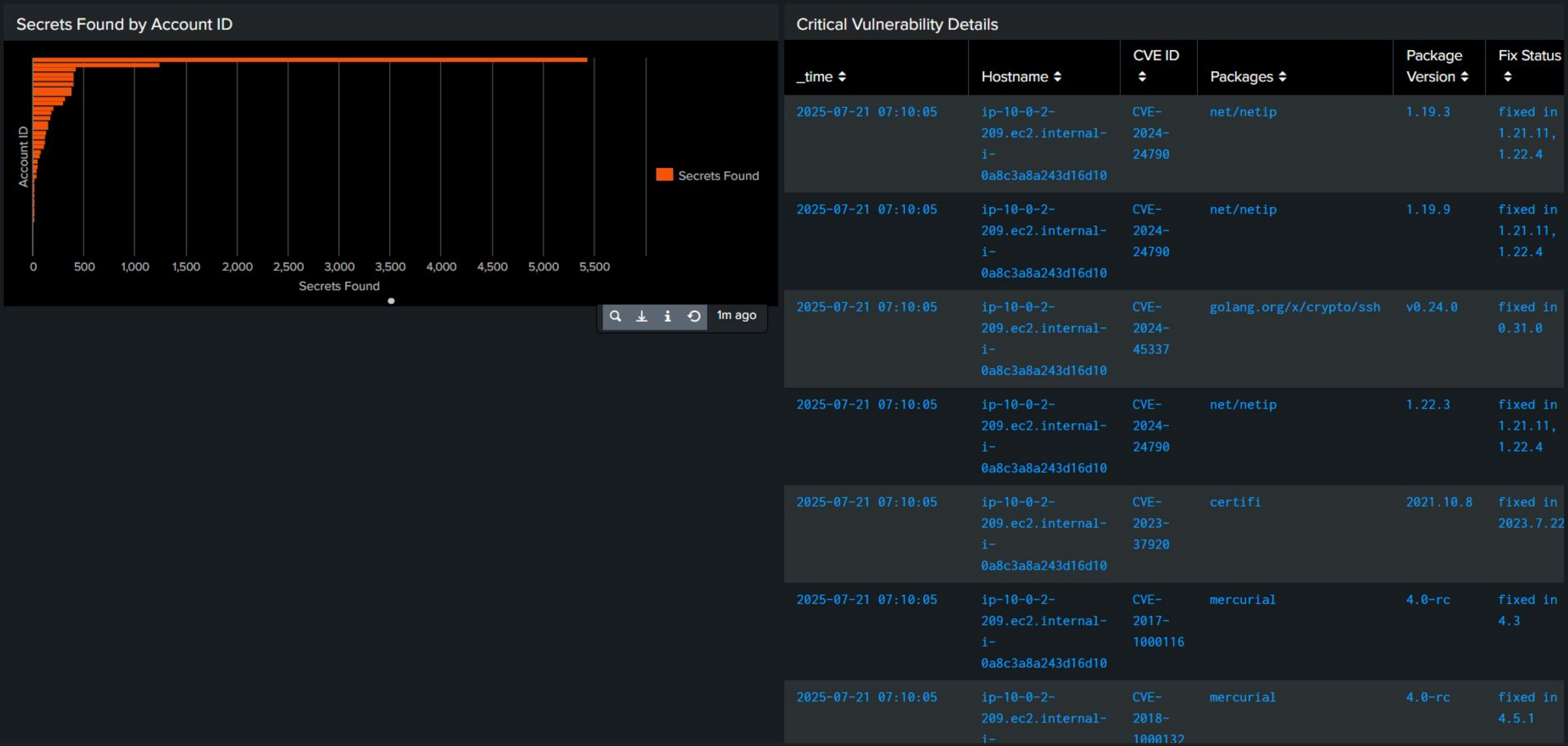
Vulnerabilities with High and Medium Severities and Their Fix Status

Account ID ⬍	Description ⬍	Fix Status ⬍	Severity ⬍
107947027614	A stack buffer overflow was found in Internationl components for unicode (ICU). While running the genrb binary, the \'subtag\' struct overflowed at the SRBRoot::addTag function. This issue may lead to memory corruption and local arbitrary code execution.	fixed in 50.2-4.amzn2.0.2	high
107947027614	Perl threads have a working directory race condition where file operations may target unintended paths. If a directory handle is open at thread creation, the process-wide current working directory is temporarily changed in order to cloneu00a0that handle for the new thread, which is visible from any third (oru00a0more) thread already running. This may lead to unintended operationsu00a0such as loading code or accessing files from unexpected locations,u00a0which a local attacker may be able to exploit. The bug was introduced in commitu00a011a11ecf4bea72b17d250cfb43c897be1341861e and released in Perl version 5.13.6	fixed in 5.16.3-299.amzn2.0.3	high
107947027614	SSH servers which implement file transfer protocols are vulnerable to a denial of service attack from clients which complete the key exchange slowly, or not at all, causing pending content to be read into memory, but never transmitted.	fixed in 3.3.2299.0-1.amzn2	high
107947027614	setuptools is a package that allows users to download, build, install, upgrade, and uninstall Python packages. A path traversal vulnerability in `PackageIndex` is present in setuptools prior to version 78.1.1. An attacker would be allowed to write files to arbitrary locations on the filesystem with the permissions of the process running the Python code, which could escalate to remote code execution depending on the context. Version 78.1.1 fixes the issue.	fixed in 49.1.3-1.amzn2.0.6	high
107947027614	The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.	fixed in 1.2.4-3.amzn2	high
107947027614	(CIS_Amazon_Linux2_1.0.0 - 4.1.18) Ensure the audit configuration is immutable		high
107947027614	(CIS_Amazon_Linux2_1.0.0 - 4.1.17) Ensure kernel module loading and unloading is collected		high
107947027614	(CIS_Amazon_Linux2_1.0.0 - 4.1.13) Ensure successful file system mounts are collected		high
107947027614	(CIS_Amazon_Linux2_1.0.0 - 4.1.17) Ensure kernel module loading and unloading is collected		high
107947027614	(CIS_Amazon_Linux2_1.0.0 - 4.1.15) Ensure changes to system administration scope (sudoers) is collected		high



Top 10 CVEs

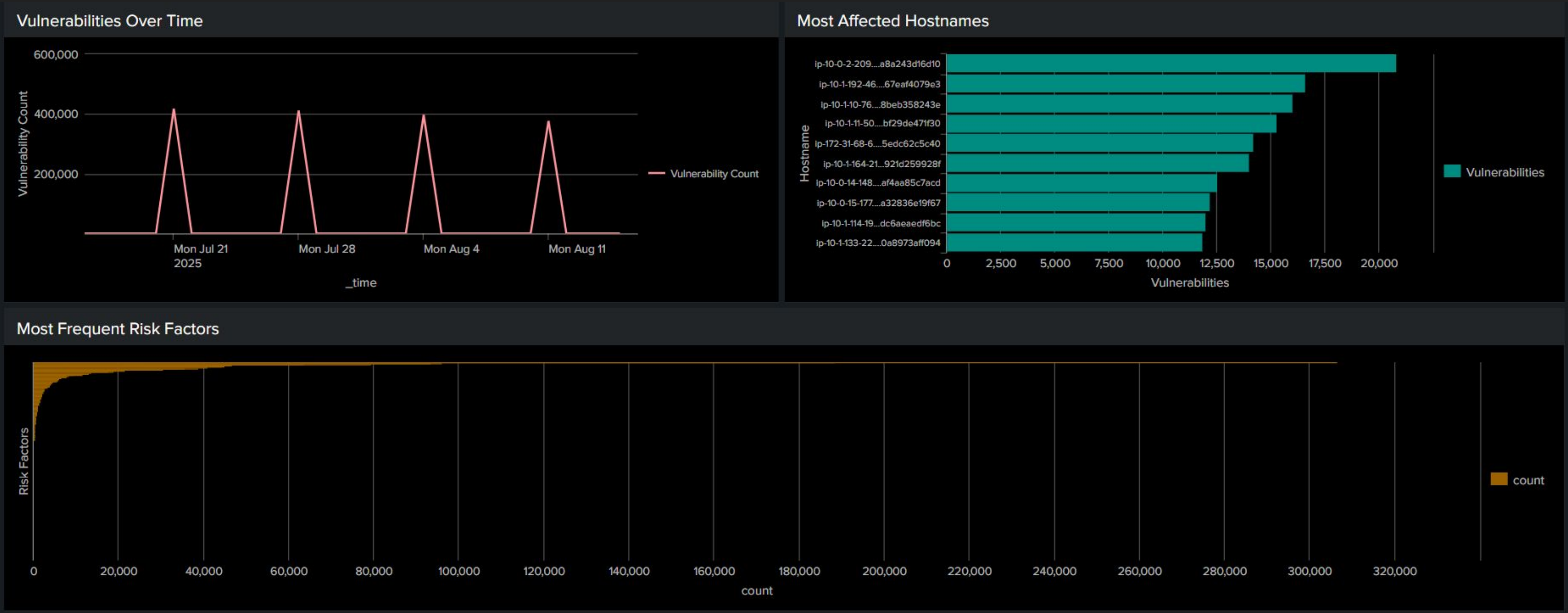
Top Vulnerable Packages



Secrets Found by Account ID

Critical Vulnerability Details

_time	Hostname	CVE ID	Packages	Package Version	Fix Status
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2024-24790	net/netip	1.19.3	fixed in 1.21.11, 1.22.4
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2024-24790	net/netip	1.19.9	fixed in 1.21.11, 1.22.4
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2024-45337	golang.org/x/crypto/ssh	v0.24.0	fixed in 0.31.0
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2024-24790	net/netip	1.22.3	fixed in 1.21.11, 1.22.4
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2023-37920	certifi	2021.10.8	fixed in 2023.7.22
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-0a8c3a8a243d16d10	CVE-2017-1000116	mercurial	4.0-rc	fixed in 4.3
2025-07-21 07:10:05	ip-10-0-2-209.ec2.internal-i-	CVE-2018-1000132	mercurial	4.0-rc	fixed in 4.5.1



Vulnerabilities Over Time

Most Affected Hostnames

ip-10-0-2-209....a8a243d16d10
ip-10-1-192-46....67eaf4079e3
ip-10-1-10-76....8beb358243e
ip-10-1-11-50....bf29de471f30
ip-172-31-68-6....5edc62c5c40
ip-10-1-164-21...921d259928f
ip-10-0-14-148....af4aa85c7acd
ip-10-0-15-177....a32836e19f67
ip-10-1-114-19...dc6aeaedf6bc
ip-10-1-133-22....0a8973aff094
Hostname
0
2,500
5,000
7,500
10,000
12,500
15,000
17,500
20,000
Vulnerabilities
Vulnerabilities

Most Frequent Risk Factors