NLP: Text Summarization With Python

Setting Up A Status Page To Monitor Cloud Infrastructure

₹120
ISSN-2456-4885

OpenSource

THE COMPLETE MAGAZINE ON OPEN SOURCE

ForYou

Volume: 13 | Issue: 05 | Pages: 100 | March 2025

An EFY GROUP Publication

Intelligent Computing Is On The Rise

MLOps Vs AIOps: What, Where, And Why

Building Machine Learning Models With Scikit-learn

Medallion Architecture: Helping Develop Agentic AI Solutions

"Open source networking solutions accelerate innovation"

–Ashay Krishna, Director Of Engineering, Microsoft

SageMath: Deeper Insights Into Cybersecurity

Yandex releases Perforator, a monitoring tool for servers

Yandex has released Perforator, an open source tool for real-time monitoring and analysis of servers and applications. It helps developers identify resource-intensive code sections and provides statistics for optimisation. By detecting inefficiencies and supporting profile-guided optimisation, Perforator enables businesses to manually optimise applications and lower infrastructure costs by up to 20%.

Perforator allows businesses to optimise code, reduce server load, and lower equipment and energy costs. It is useful for large data centres, corporations, and startups with limited resources. Instead of investing in new hardware, companies can use Perforator to existing infrastructure. It has been used in services for over a year and is available globally. Companies can deploy it on their own servers, reducing dependence on external cloud providers while maintaining data control. Organisations with strict security requirements can benefit from its deployment in closed environments.

Perforator helps reduce infrastructure costs, freeing resources for further growth. It supports A/B testing for performance analysis and optimisation. By open sourcing it, Yandex aims to foster community collaboration in system technology development.

Its source code is available on GitHub along with other Yandex open source projects, including YaFSDP, AQLM, and YTsaurus. Future updates will enhance Python and Java integration and provide more precise event analysis.

a cult following. When Fitbit was later acquired by Google in 2021, PebbleOS became part of Google's portfolio.

Even though official support ended years ago, thousands of Pebble watches remain in use, cherished for their simplicity, long battery life, and unique features.

Google's decision to release the majority of PebbleOS's source code is seen as a goodwill gesture toward the devoted Pebble community. The open source release includes PebbleOS's core components, supporting key features like notifications, media controls, fitness tracking, and customisable apps. Built on FreeRTOS for low-power ARM Cortex-M microcontrollers, PebbleOS remains highly optimised for long battery life and e-ink displays—a design approach that is rare in today's smartwatch market.

"It's important to note that some proprietary code was removed from this codebase, particularly for chipset support and the Bluetooth stack," explained Google. "This means the code being released contains all the build system files (using the Waf build system), but it will not compile or link as released."

OpenSSH patches critical vulnerabilities

OpenSSH has released security updates to patch two critical vulnerabilities that could allow attackers to execute man-in-the-middle (MitM) attacks and cause denial-of-service (DoS) disruptions. One of the flaws had remained undetected for over a decade.

Security researchers at Qualys discovered the vulnerabilities and demonstrated their exploitability to OpenSSH maintainers. The flaws impact OpenSSH, the widely used open source implementation of the Secure Shell (SSH) protocol, which provides encrypted remote access, secure file transfers, and tunnelling over untrusted networks.

The vulnerability, tracked as CVE-2025-26465, was introduced in OpenSSH 6.8p1 in December 2014, meaning it has been present for over ten years. It affects OpenSSH clients when the *VerifyHostKeyDNS* option is enabled, allowing attackers to intercept SSH connections and inject rogue keys. According to Qualys, the attack succeeds whether *VerifyHostKeyDNS* is set to 'yes' or 'ask' (default: 'no'), requiring no user interaction and not depending on the presence of SSHFP records in DNS.

By intercepting an SSH session and presenting a large SSH key with excessive certificate extensions, attackers can force an out-of-memory error during host key verification. This manipulation tricks the client into accepting a rogue server's key, enabling credential theft, command injection, and data exfiltration.

A separate DoS vulnerability could allow attackers to overwhelm SSH servers with malicious connections, exhausting system resources and causing service disruptions.

To address these vulnerabilities, OpenSSH has released version 9.9p2, which patches both issues. Security experts recommend that all users and system administrators upgrade immediately.

Additionally, users are advised to disable *VerifyHostKeyDNS* unless absolutely necessary, as it provides an attack vector for MitM exploits. Manual key fingerprint verification is the recommended alternative. Also, connection rate limits should be enforced to mitigate potential DoS attacks. Monitoring SSH traffic for unusual patterns can help detect early signs of an attack.

These vulnerabilities highlight the importance of ongoing security assessments, even for long-standing software, as critical flaws can remain unnoticed for years.

The Linux Foundation to launch C4SB Foundation for open data standards in smart buildings

The Linux Foundation has announced plans to integrate the Coalition for Smarter Buildings (C4SB) and establish the C4SB Foundation, a new initiative dedicated to advancing open data standards and open source solutions for smart buildings. This move aims to foster collaboration among industry leaders, enabling more efficient, sustainable, and intelligent building management worldwide.

Originally founded in 2021, C4SB is a non-profit organisation that unites technology innovators, building owners, and domain experts to accelerate smart building adoption. By joining the Linux Foundation, [illegible] enhance its ability to develop open standards and software [illegible] interoperability and efficiency in real estate operations. The [illegible]ation will focus on creating open interoperability between [illegible]omation systems and digital real estate applications, improving [illegible]al efficiency through standardised data exchange and automation, enhancing occupant experiences by leveraging smarter, more responsive building technologies, and advancing sustainability by streamlining energy and resource management.

Jim Zemlin, executive director of the Linux Foundation, emphasised the importance of this move, stating, "Open source collaboration is crucial to driving innovation across industries, and the move of the C4SB to the Linux Foundation underscores the potential for open source in real estate. By uniting key players in the building and real estate sectors, we are creating a shared framework for interoperability while advancing sustainability and digital transformation in smart buildings."

Rick Justis, executive director of C4SB, highlighted the significance of this initiative, saying, "The fragmented data landscape in real estate and building management has long been a challenge. By uniting open standards and open source software under the Linux Foundation, C4SB will empower stakeholders to achieve higher efficiency, transparency, and sustainability in the built environment."

The C4SB Foundation is inviting real estate professionals, building owners, facilities managers, and technology providers to participate in shaping the future of smart buildings. For more information and membership details, visit the C4SB website at *https://www.c4sb.org/*.

For more news, visit *www.opensourceforu.com*

Apache Software Foundation announces new Top-Level Projects

The Apache Software Foundation (ASF) has announced that Apache Answer and Apache StreamPark have graduated from incubation and are now recognised as Top-Level Projects (TLP). This milestone highlights the maturity, stability, and community engagement of both projects as they continue to evolve under ASF's stewardship.

Apache Answer is an open source Q&A platform designed to help organisations build and maintain knowledge bases while fostering collaborative communities. It enables teams to efficiently create, share, and discover knowledge in a structured manner. "Apache Answer's graduation as a Top-Level Project marks a significant milestone in our journey," said Ning Qi, vice president of Apache Answer. "This achievement reflects the dedication of our community and the maturity of our platform in providing a Q&A platform solution for knowledge management and community engagement." More details about the project [illegible] at *answer.apache.org*.

Apache StreamPark is an [illegible] streaming application develop[illegible] and operation platform that suppo[illegible] Flink and Apache Spark, providing full lifecycle support for stream processing applications. "Becoming an Apache Software Foundation Top-Level Project is a significant milestone and one that would not be possible without the dedication and hard work of the StreamPark community," said Huajie Wang, vice president of Apache StreamPark. "We look forward to continued technical and community growth under the ASF's stewardship." More information on StreamPark is available at *streampark.apache.org*.

ASF's incubation process provides open source projects with essential mentorship and resources to help them establish strong, sustainable communities. By officially graduating to Top-Level Project status, Apache Answer and Apache StreamPark have demonstrated their ability to thrive independently while embracing ASF's commitment to open collaboration and long-term project sustainability.