USN-4761-1: Git vulnerability

Matheus Tavares discovered that Git incorrectly handled delay-capable
clean/smudge filters when being used on case-insensitive filesystems. A
remote attacker could possibly use this issue to execute arbitrary code.

Industry-Wide Initiative to Support Open Source Security Gains New Commitments

Open Source Security Foundation adds new members, Citi, Comcast, DevSamurai, HPE, Mirantis and Snyk

SAN FRANCISCO, Calif., March 9, 2021 – OpenSSF, a cross-industry collaboration to secure the open source ecosystem, today announced new membership commitments to advance open source security education and best practices. New members include Citi, Comcast, DevSamurai, Hewlett Packard Enterprise (HPE), Mirantis, and Snyk.

Open source software (OSS) has become pervasive in data centers, consumer devices and services, representing its value among technologists and businesses alike. Because of its development process, open source has a chain of contributors and dependencies before it ultimately reaches its end users. It is important that those responsible for their user or organization's security are able to understand and verify the security of this dependency supply chain.

"Open source software is embedded in the world's technology

infrastructure and warrants our dedication to ensuring its security," said Kay Williams, Governing Board Chair, OpenSSF, and Supply Chain Security Lead, Azure Office of the CTO, Microsoft. "We welcome the latest OpenSSF new members and applaud their commitment to advancing supply chain security for open source software and its technology and business ecosystem."

The OpenSSF is a cross-industry collaboration that brings together technology leaders to improve the security of OSS. Its vision is to create a future where participants in the open source ecosystem use and share high quality software, with security handled proactively, by default, and as a matter of course. Its working groups include Securing Critical Projects, Security Tooling, Identifying Security Threats, Vulnerability Disclosures, Digital Identity Attestation, and Best Practices.

OpenSSF has more than 35 members and associate members contributing to working groups, technical initiatives and governing board and helping to advance open source security best practices. For more information on founding and new members, please visit: https://openssf.org/about/members/

Membership is not required to participate in the OpenSSF. For more information and to learn how to get involved, including information about participating in working groups and advisory forums, please visit https://openssf.org/getinvolved.

New Member Comments

Citi

"Working with the open source community is a key component in our security strategy, and we look forward to supporting the OpenSSF in its commitment to collaboration," said Jonathan Meadows, Citi's Managing Director for Cloud Security Engineering.

Comcast

“Open source software is a valuable resource in our ongoing work to create and continuously evolve great products and experiences for our customers, and we know how important it is to build security at every stage of development. We’re honored to be part of this effort and look forward to collaborating,” said Nithya Ruff, head of Comcast Open Source Program Office.

DevSamurai

“We are living in an interesting era, in which new IT technologies are changing all aspects of our lives everyday. Benefits come with risks, that can’t be truer with open source software. Being a part of OpenSSF we expect to learn from and contribute to the community, together we strengthen security and eliminate risks throughout the software supply chain,” Said Tam Nguyen, head of DevSecOps at DevSamurai.

Mirantis

“As open source practitioners from our very founding, Mirantis has demonstrated its commitment to the values of transparency and collaboration in the open source community,” said Chase Pettet, lead product security architect, Mirantis. “As members of the OpenSSF, we recognize the need for cross-industry security stakeholders to strengthen each other. Our customers will continue to rely on open source for their safety and assurance, and we will continue to support the development of secure open solutions.”

Snyk

“As the number of digital transformation projects has exploded the world over, the mission of the Open Source Security Foundation has never been more critical than it is today,” said Geva Solomonovich, CTO, Global Alliances, Snyk. “Snyk is thrilled to become an official Foundation member, and we look forward to working with the entire community to together push

the industry to make all digital environments safer.”

About the Open Source Security Foundation (OpenSSF)

Hosted by the Linux Foundation, the OpenSSF (launched in August 2020) is a cross-industry organization that brings together the industry’s most important open source security initiatives and the individuals and companies that support them. It combines the Linux Foundation’s Core Infrastructure Initiative (CII), founded in response to the 2014 Heartbleed bug, and the Open Source Security Coalition, founded by the GitHub Security Lab to build a community to support the open source security for decades to come. The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.

About the Linux Foundation

Founded in 2000, the Linux Foundation is supported by more than 1,000 members and is the world’s leading home for collaboration on open source software, open standards, open data, and open hardware. Linux Foundation’s projects are critical to the world’s infrastructure including Linux, Kubernetes, Node.js, and more. The Linux Foundation’s methodology focuses on leveraging best practices and addressing the needs of contributors, users and solution providers to create sustainable models for open collaboration. For more information, please visit us at linuxfoundation.org.

###

Media Contact

Jennifer Cloer

for the Linux Foundation

503-867-2304

jennifer@storychangesculture.com

The post Industry-Wide Initiative to Support Open Source Security Gains New Commitments appeared first on Linux Foundation.

Linux Foundation Announces Free sigstore Signing Service to Confirm Origin and Authenticity of Software

Red Hat, Google and Purdue University lead efforts to ensure software maintainers, distributors and consumers have full confidence in their code, artifacts and tooling

SAN FRANCISCO, Calif., March 9, 2021 – The Linux Foundation, the nonprofit organization enabling mass innovation through open source, today announced the sigstore project. sigstore improves the security of the software supply chain by enabling the easy adoption of cryptographic software signing backed by transparency log technologies.

sigstore will empower software developers to securely sign software artifacts such as release files, container images and binaries. Signing materials are then stored in a tamper-proof public log. The service will be free to use for all developers

and software providers, with the sigstore code and operation tooling developed by the sigstore community. Founding members include Red Hat, Google and Purdue University.

“sigstore enables all open source communities to sign their software and combines provenance, integrity and discoverability to create a transparent and auditable software supply chain,” said Luke Hinds, Security Engineering Lead, Red Hat office of the CTO. “By hosting this collaboration at the Linux Foundation, we can accelerate our work in sigstore and support the ongoing adoption and impact of open source software and development.”

Understanding and confirming the origin and authenticity of software relies on an often disparate set of approaches and data formats. The solutions that do exist, often rely on digests that are stored on insecure systems that are susceptible to tampering and can lead to various attacks such as swapping out of digests or users falling prey to targeted attacks.

“Securing a software deployment ought to start with making sure we’re running the software we think we are. Sigstore represents a great opportunity to bring more confidence and transparency to the open source software supply chain,” said Josh Aas, executive director, ISRG | Let’s Encrypt.

Very few open source projects cryptographically sign software release artifacts. This is largely due to the challenges software maintainers face on key management, key compromise / revocation and the distribution of public keys and artifact digests. In turn, users are left to seek out which keys to trust and learn steps needed to validate signing. Further problems exist in how digests and public keys are distributed, often stored on websites susceptible to hacks or a README file situated on a public git repository. sigstore seeks to solve these issues by utilization of short lived ephemeral keys with a trust root leveraged from an open and auditable public

transparency logs.

“I am very excited about the prospects of a system like sigstore. The software ecosystem is in dire need of something like it to report the state of the supply chain. I envision that, with sigstore answering all the questions about software sources and ownership, we can start asking the questions regarding software destinations, consumers, compliance (legal and otherwise), to identify criminal networks and secure critical software infrastructure. This will set a new tone in the software supply chain security conversation,” said Santiago Torres-Arias, Assistant Professor of Electrical and Computer Engineering, University of Purdue / in-toto project founder.

“sigstore is poised to advance the state of the art in open source development,” said Mike Dolan, senior vice president and general manager of Projects at the Linux Foundation. “We are happy to host and contribute to work that enables software maintainers and consumers alike to more easily manage their open source software and security.”

“sigstore aims to make all releases of open source software verifiable, and easy for users to actually verify them. I’m hoping we can make this easy as exiting vim,” Dan Lorenc, Google Open Source Security Team. “Watching this take shape in the open has been fun. It’s great to see sigstore in a stable home.”

For more information and to contribute, please visit: https://sigstore.dev

About the Linux Foundation

Founded in 2000, the Linux Foundation is supported by more than 1,000 members and is the world’s leading home for collaboration on open source software, open standards, open data, and open hardware. Linux Foundation’s projects are critical to the world’s infrastructure including Linux,

Kubernetes, Node.js, and more. The Linux Foundation's methodology focuses on leveraging best practices and addressing the needs of contributors, users and solution providers to create sustainable models for open collaboration. For more information, please visit us at linuxfoundation.org.

###

Media Contact

Jennifer Cloer

for Linux Foundation

503-867-2304

jennifer@storychangesculture.com

The post Linux Foundation Announces Free sigstore Signing Service to Confirm Origin and Authenticity of Software appeared first on Linux Foundation.

USN-4758-1: Go vulnerability

It was discovered that Go applications incorrectly handled uploaded content. If
a user were tricked into visiting a malicious page, a remote attacker could
exploit this with a crafted file to conduct cross-site scripting (XSS) attacks.

USN-4760-1: libzstd vulnerabilities

It was discovered that libzstd incorrectly handled file permissions. A
local attacker could possibly use this issue to access certain files,
contrary to expectations.