- Risk Management
- Compliance
- Privacy
- Supply Chain
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Identity & Access

GitHub Encourages Users to Adopt Two-Factor Authentication

By Ionut Arghire on August 19, 2021

Share Tweet 推荐 10 RSS

Software repository platform GitHub is once again encouraging users to enable two-factor authentication (2FA) to better secure their accounts.

The Microsoft-owned hosting service has had support for 2FA for eight years, and is now pushing for a wider use of the feature after it stopped accepting account passwords for authenticating Git operations.

Initially announced in July 2020 and in effect starting August 13, 2021, the change requires the use of token-based authentication (personal access token, SSH keys, or an OAuth or GitHub App installation token) for all Git operations.

Following this switch, GitHub is now encouraging all of its users to enable 2FA to better protect their accounts, once again reminding them of the benefits of this feature, such as better protection against phishing and other types of attacks.

GitHub users who haven’t yet enabled 2FA on their accounts but wish to do so can use physical security keys for that, but also virtual security keys built into personal devices, Time-based One-Time Password (TOTP) authenticator apps, or SMS.

For more than half a decade, SMS has been considered an insecure 2FA option, and GitHub is strongly recommending the use of security keys or TOTPs instead, if possible.

“SMS-based 2FA does not provide the same level of protection, and it is no longer recommended under NIST 800-63B. The strongest methods widely available are those that support the emerging WebAuthn secure authentication standard. These methods include physical security keys as well as personal devices that support technologies such as Windows Hello or Face ID/Touch ID,” GitHub notes.

Users who protect their accounts with a security key can also digitally sign git commits with a GPG key stored on that security key, the software hosting platform explains.

Related: Why Are Users Ignoring Multi-Factor Authentication?

Related: New 'Allstar' App Enforces Security Best Practices for GitHub Projects

Related: GitHub Updates Policies on Vulnerability Research, Exploits

Share Tweet 推荐 10 RSS

Ionut Arghire is an international correspondent for SecurityWeek.
Previous Columns by Ionut Arghire:
CISA Issues Guidance on Protecting Data From Ransomware
Third-Party Patches Available for More PetitPotam Attack Vectors
Hackers Steal $97 Million from Japanese Crypto-Exchange Liquid
Cisco: Critical Flaw in Older SMB Routers Will Remain Unpatched
Cyberattack Forces Memorial Health System to Cancel Surgeries, Divert Patients

Tags:
NEWS & INDUSTRY Identity & Access Management & Strategy

Search

Get the Daily Briefing

BRIEFING

Business Email Address Subscribe