

Security Newsletter

27 May 2019

[Subscribe to this newsletter](#)

Github provides a new tool to secure your code



According to GitHub, ninety-nine percent of new software projects depend on open source code. This extensive code reuse helps everyone build better software faster than ever before, but it also puts us all at risk of distributing security vulnerabilities from our dependencies. It's more important than ever that every developer becomes a security developer—that they responsibly disclose vulnerabilities and patch vulnerable code quickly.

On the 23rd, GitHub announced several new security features designed to make it easier for developers to secure their code.

Enhanced security vulnerability alerts: since GitHub sent almost 27 million security alerts for vulnerable dependencies in .NET, Java, JavaScript, Python and Ruby

Dependency insights: a tool that gives an overview of the dependencies of the projects and their security state to assess your project exposure.

Token scanning: scans your repository to find AWS, GCP, Twilio and other tokens to avoid data breaches.

Automated security fixes: when your project uses an outdated and unsecured dependency, an automated pull request is created with the commit to update the version.

A lot of good tools to implement internally to protect your company.

[Read More on GitHub announce](#)

Massive leak of hundreds of millions of title insurance records



On Friday, independent security journalist Brian Krebs revealed that the real estate and title insurance giant First American had 885 million sensitive customer financial records, going back to 2003, exposed on its website for anyone to access.

Krebs reports that the exposed records included Social Security numbers, driver's license images, bank account numbers and statements, mortgage and tax documents, and wire transaction receipts—an absolute treasure trove for any scammer or identity thief.

The hack was simple: an attacker who figured out the format of the company's document URLs could have input any "record number" they wanted—beginning with "000000075," according to Krebs—and pull up the documents associated with that customer case. First American took down the site that populated the records at 2 pm ET on Friday.

The First American exposure is a major incident, because it underscores just how little progress many institutions have made on locking down customer data. Perfect security is impossible, but the stakes are incredibly high and many large organizations still overlook basic errors.

[Read More on Wired](#)

[Read more on Krebs on Security](#)

More #News

- [Google Stored G Suite Users' Passwords in Plain-Text](#)
- [The Most Expensive Lesson Of My Life: Details of SIM port hack](#)
- [Windows ATP For macOS](#)
- [Georgia Supreme Court Rules that State Has No Obligation to Protect Personal Information](#)
- [Microsoft Brings Hardware-Based Isolation to Chrome, Firefox](#)
- [Researcher Drops 3 Separate 0-Day Windows Exploits in 24 Hours](#)
- [NATO Warns Russia of 'Full Range' of Responses to Cyberattack](#)
- [Comodo Issued Most Certificates for Signed Malware on VirusTotal](#)
- [Authorities Take Down Cryptocurrency Mixing Service Bestmixer.io](#)
- [Mobile Chrome, Safari and Firefox failed to show phishing warnings for more than a year](#)
- [PoC Exploits Created for Wormable Windows RDS Flaw](#)
- [LinkedIn Allowed TLS Certificate to Expire—Again](#)
- [Magecart Skimmer Poses as Payment Service Provider](#)
- [One Year On, EU Has 145,000 Data Law Complaints](#)
- [New unpatched macOS Gatekeeper Bypass Published Online](#)

#Patch Time!

- [WebLogic Deserialization Remote Code Execution Vulnerability](#)

#Tech and #Tools

- [XSS without parentheses and semi-colons](#)
- [AWS Security Incident Response](#)
- [Microsoft Brings Hardware-Based Isolation to Chrome, Firefox and Edge](#)
- [New version of OLE Tools released](#)
- [Security Features in Elasticsearch are now free](#)
- [Security Baseline for Windows 10 v1903 and Windows Server v1903](#)

We need

YOU!



Kindred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our [Cyber Security team](#)
- You prefer the blue team side? Check out our [Security analyst position](#)
- Interested in Governance, Risk and Compliance? Apply for our [Information Security Specialist role](#)

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our [career page](#).

This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>

If you no longer wish to receive this newsletter, you can [unsubscribe from this list](#)