Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 48718a1a | Oct 07, 2021, 10:43 AM

Today's Headlines:

Leading Story
- Facebook Blames Global Outage on Configuration Error

Data Breaches & Data Leaks
- Ransomware Attack on Florida Behavioral Health Service Provider Affects 19,000 Individuals

Cyber Crimes & Incidents
- Prolific Ransomware Operators Arrested in Joint Law Enforcement Action
- Text Message Giant Reveals Five-Year Breach

Vulnerabilities & Exploits
- Android October Patch Fixes Three Critical Bugs, 41 Flaws in Total

Trends & Reports
- Google Pledges $1m to Secure Open-Source Project

Privacy, Legal & Regulatory
- Facebook Whistleblower to Testify Before Senate

Upcoming Health-ISAC Events
- Health-ISAC Monthly Threat Brief – October 28, 2021, 12:00 PM Eastern

Additional Info

Leading Story

Facebook Blames Global Outage on Configuration Error

Summary
- Facebook has apologized for a major global outage that left users unable to access the social network and other platforms for hours, blaming the incident on a configuration error.

Analysis & Action

The outage began at around 11:40 Eastern Time on Monday morning, October 4, 2021, and lasted well into the evening of the same day, affecting Facebook, Facebook Messenger, Instagram, and WhatsApp.

The issue appears to have stemmed from an update to the firm's Border Gateway Protocol (BGP) records. It's a mechanism to exchange routing information between autonomous systems (AS) on the internet, explained Cloudflare in a technical blog about the incident.

Although some commentators had speculated foul play, the cause of the outage appears to be human error. Facebook vice president of infrastructure said that no user data was compromised and that the root cause of the issue was a faulty configuration change.

The full Cloudflare technical report can be accessed here.

Data Breaches & Data Leaks

Ransomware Attack on Florida Behavioral Health Service Provider Affects 19,000 Individuals

Summary

- Non-profit behavioral health service provider Directions for Living has found itself the victim of a ransomware attack which occurred on July 17, 2021.

Analysis & Action

Upon detection of the attack, law enforcement was notified and third-party computer forensics experts were engaged to investigate the scope of the attack and assist with remediation efforts. The investigation concluded on August 30, 2021 and confirmed that breached servers contained personal and protected health information of current and former clients.

Directions for Living have stated that no evidence has been found to indicate any actual or attempted misuse of protected health information. The breach report submitted to the US Department of Health and Human Services' Office for Civil Rights indicates the protected health information of 19,494 individuals was stored on the affected servers.

Cyber Crimes & Incidents

Prolific Ransomware Operators Arrested in Joint Law Enforcement Action

Summary

- A coordinated law enforcement action has led to the arrest of two ransomware operators in Ukraine, Europol has reported.

Analysis & Action

The operation was coordinated between the French National Gendarmerie, the Ukrainian National Police and the United States Federal Bureau of Investigation (FBI) in conjunction with Europol and INTERPOL on September 28. While neither the individuals nor the gang they allegedly belong to were named, Europol said they were also known for their ransom demands between €5m and €70m.

The Ukrainian authorities stated that the suspects were responsible for attacks against over 100 worldwide organizations, causing more than $150 million in damages. As well as the two arrests, the joint law enforcement action resulted in seven property searches, seizure of $375,000 in cash, seizure of two luxury vehicles worth €217,000 and asset freezing of $1.3m in cryptocurrencies.

Text Message Giant Reveals Five-Year Breach

Summary

- A major telecoms service provider has revealed it was the victim of a five-year breach impacting hundreds of customers.

Analysis & Action

Syniverse routes text messages for hundreds of global telco customers, claiming to reach more people and devices than anyone on Earth. However, in a filing with the US Securities and Exchange Commission (SEC) ahead of the firm going public via a merger with a special purpose acquisition company, it admitted to secretly discovering a major incident in May of 2021.

Unauthorized access to its operational and IT systems was subsequently found to have been ongoing since May of 2016.

Syniverse's investigation revealed that the individual or organization gained unauthorized access to databases within its network on several occasions, the filing reported. It's unclear exactly what information the attackers would have gained access to with the compromise, but it could theoretically include metadata or even the content of text messages, including one-time passcodes, which could unlock two-factor authentication-protected accounts.

The firm claims to process over 740 billion messages every year for over 300 global mobile operators.

Vulnerabilities & Exploits

Android October Patch Fixes Three Critical Bugs, 41 Flaws in Total

Summary

- Google has released the Android October security updates, addressing 41 vulnerabilities, all ranging between high and critical severity.

Analysis & Action

The high-severity flaws fixed this month concern denial of service, elevation of privilege, remote code execution, and information disclosure issues. However, none of the 41 flaws addressed this month have been reported to be under active exploitation in the wild, so there should be no working exploits for them circulating out there.

Older devices that are no longer supported with Android security updates now have an increased attack surface, as some of the vulnerabilities fixed this month are new candidates for threat actors to create working exploits in the future.

Trends & Reports

Google Pledges $1m to Secure Open-Source Project

Summary

- Google has announced financial backing for a new initiative designed to incentivize proactive security improvements to open-source code.

Analysis & Action

Unlike bug bounty programs which offer financial rewards to researchers who discover critical software bugs, the Secure Open Source (SOS) project will do the same for developers whose work prevents major vulnerabilities from initially appearing.

The selection process for in-scope projects will take into account NIST guidelines and the new US Presidential executive order on cybersecurity, as well as criteria such as how many users will be affected, and how serious an impact a compromise would have.

The initial list of projects includes software supply chain improvements, as a recent report from Sonatype revealed a 650% year-on-year increase in upstream supply chain attacks impacting open-source software components.

We envision the SOS pilot program as the starting point for future efforts that will hopefully bring together other large organizations and turn it into a sustainable, long-term initiative, Google stated.

Privacy, Legal & Regulatory

Facebook Whistleblower to Testify Before Senate

Summary

- A former Facebook employee is to appear before a US Senate subcommittee tomorrow after blowing the whistle on the company's alleged prioritization of profit above user welfare.

Analysis & Action

Frances Haugen, a data scientist, revealed earlier this week that she leaked internal research carried out by Facebook and reported it to the Wall Street Journal. This research formed the basis of an investigative series named The Facebook Files, which the Journal has been reporting for the past three weeks.

Among the claims made by the Journal are that Facebook identified negative effects that its platform was having upon its users but didn't take any action to fix the problems. It is further alleged that while claiming to treat all its users equally, Facebook allowed certain high-profile users to post content including harassment and incitement to violence.

On October 5, 2021, Haugen will testify before a US Senate subcommittee in a hearing on Facebook's research into Instagram's effect on the mental health of young people. Two members of the European Parliament have also called for an investigation to be launched into the social media company.

Reference | References

Info Security Magazine
Info Security Magazine
Health-ISAC
Info Security Magazine
cloudflare
Bleeping Computer
Health-ISAC
Info Security Magazine
HIPAA Journal
Info Security Magazine

Tags

Daily Cyber Headlines, DCH
