

## Contents

**01 Patches Notes**

---

**02 Cyber Attack**

---

**03 Malware and Vulnerabilities**

---

**04 Cyber-Tech**

---

“

**CYBER-SECURITY  
IS MUCH MORE  
THAN A MATTER  
OF IT.** — Stephane Nappo

# Patches Notes

---

## APPLE EMERGENCY ZERO-DAY FIX

---

- The vulnerability was apparently found in the IOMobileFrameBuffer kernel code, a component that helps userland applications (in other words, unprivileged software) to configure and use your device's or computer's display.
- These include elevation of privilege (EoP), in which an otherwise uninteresting app gains the same level of power as the operating system itself, and remote code execution (RCE), in which an otherwise innocent operation, such as viewing a web page or opening an image, can trick the kernel into running completely untrusted code that did not originate with Apple. [↗](#)

## ATLASSIAN ASKS CUSTOMERS TO PATCH CRITICAL JIRA VULNERABILITY

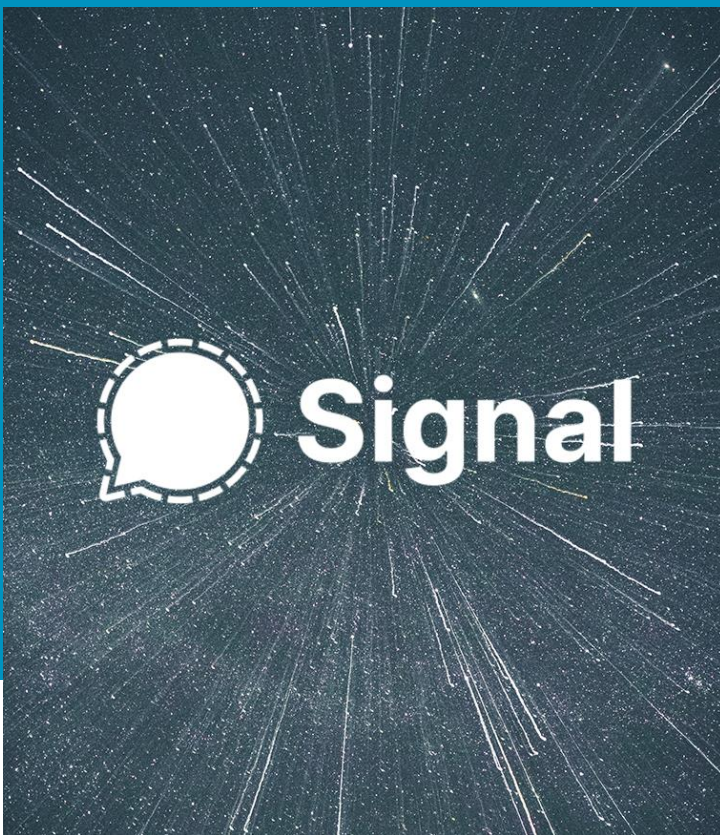
---

- Atlassian is prompting its enterprise customers to patch a critical vulnerability in many versions of its Jira Data Center and Jira Service Management Data Center products.
- The vulnerability tracked as CVE-2020-36239 can give remote attackers arbitrary code execution abilities, due to a missing authentication flaw in Jira's implementation of Ehcache, an open-source component. [↗](#)

## SIGNAL FIXES BUG THAT SENT RANDOM IMAGES TO WRONG CONTACTS

---

- Signal has fixed a serious bug in its Android app that, in some cases, sent random unintended pictures to contacts without an obvious explanation.
- When sending an image using the Signal Android app to one of your contacts, the contact would occasionally receive not just the selected image, but additionally a few random, unintended images, that the sender had never sent out. [↗](#)



## NORTHERN IRELAND SUSPENDS VACCINE PASSPORT SYSTEM AFTER DATA LEAK

- Following a data exposure event, Northern Ireland's Department of Health (DoH) has temporarily stopped its COVID-19 vaccination certification online service.
- This is a distinct system from the NHS COVID Pass used in England and Wales, as well as a comparable "vaccine passport" service used by Public Health Scotland.



# CYBER ATTACKS



## KASEYA OBTAINS UNIVERSAL DECRYPTOR FOR REvil RANSOMWARE


- The attacks, which targeted now-patched zero-day vulnerabilities in the Kaseya Virtual System/Server Administrator (VSA) platform, impacted Kaseya customers in 22 countries who were using the on-premises version of the platform, many of whom are managed service providers (MSPs) who use VSA to manage the networks of other businesses.
- Following the attacks, the REvil gang (aka Sodinokibi) requested \$70 million for a universal public decryption key that will compensate all victims — a figure that one researcher claims was finally reduced to \$50 million.



## OVER HALF A MILLION CYBERSECURITY INCIDENTS REPORTED IN INDIA

- Over 6.07 lakh cyber security incidents were observed in the country during the first half of 2021, Parliament was informed on Wednesday.
- The minister noted that the government has taken a number of measures to enhance the cyber security posture and prevent cyber-attacks, including CERT-In issuing alerts and advisories regarding latest cyber threats

# Malware and Vulnerabilities



**MACOS MALWARE STEALS TELEGRAM ACCOUNTS, GOOGLE CHROME DATA**

- Telegram instant messaging programme is one of the targeted apps. The virus generates the archive "telegram.applescript" for the Group Containers directory's "keepcoder.Telegram" subdirectory.
- XCSSET is targeting the most recent macOS version (now Big Sur) and has previously been observed to use a zero-day vulnerability to evade full disc access restrictions and avoid explicit user content. [↗](#)



## FAKE WINDOWS 11 INSTALLERS NOW USED TO INFECT YOU WITH MALWARE

- The fast change and growing usage of remote work choices, such as virtual private networks (VPNs) and cloud-based settings, has most certainly added to the load on cyber defenders who are already trying to maintain and keep up with normal software patching.
- One of the infected individuals downloaded a 1.75 GB bogus Windows 11 installer, which when run presented what seemed to be a Windows installation wizard. [↗](#)

## FBI REVEALS TOP TARGETED VULNERABILITIES OF THE LAST TWO YEARS

- CISA, the Australian Cyber Security Centre (ACSC), the National Cyber Security Centre (NCSC) of the United Kingdom, and the Federal Bureau of Investigation (FBI) also offered countermeasures to assist commercial and public sector companies in combating these vulnerabilities.
- The fast change and growing usage of remote work choices, such as virtual private networks (VPNs) and cloud-based settings, has most certainly added to the load on cyber defenders who are already trying to maintain and keep up with normal software patching. [↗](#)

## AKAMAI DNS GLOBAL OUTAGE TAKES DOWN MAJOR WEBSITES, ONLINE SERVICES

- Akamai is looking into a continuous outage that is affecting several major websites and online services, including Steam, PlayStation Network, Newegg, AWS, Amazon, Google, and Salesforce.
- The outage lasted up to an hour. The services resumed regular functioning when the software configuration upgrade was rolled back. Akamai can certify that this was not a cyberattack on their platform. [↗](#)

# CYBER TECH



## SOPHOS ACQUIRES BRAINTRACE TO SUPERCHARGE ITS THREAT DETECTION CAPABILITIES

- Sophos, which is owned by Thoma Bravo, has announced the acquisition of Braintrace, a cybersecurity firm that offers enterprises with visibility into suspicious network traffic patterns.
- The technology will also assist Sophos in collecting data from firewalls, proxies, and VPNs, allowing it to look for network traffic containing instructions for malware such as TrickBot and attackers who abuse Cobalt Strike, as well as preventing other malicious traffic that could lead to ransomware attacks. [↗](#)



## MICROSOFT TEAMS GETS MORE PHISHING PROTECTION!

- Since its debut in 2015, Safe Links has been a crucial feature in Defender for Office 365. Safe Links, at its heart, verifies URLs at the moment of click.
- Defender for Office 365 delivers complete protection against attacks such as phishing, malware, and corporate email compromise, providing administrators the tools they need not just to avoid and identify these threats, but also to analyse and remediate any problems they discover. [↗](#)

## INDIA WILL BE THE FIRST COUNTRY TO ADOPT DEFAULT SECURITY FEATURES IN O-RAN TELECOM NETWORKS.

- India supports the early implementation of default security measures in open radio access networks for telecom services.
- In the telecom sector, the O-RAN idea is similar to open-source software technologies in that any firm can utilise an open technology to create its technological solution without claiming a patent for it. [↗](#)



## ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

## SECURITY INFORMATION & EVENT MANAGEMENT



A Business's IT network is a goldmine of information and actionable data. At Infopercept we have a strong state-of-the-art SIEM implementation plan as well as valuable market insights due to years of experience in the Cybersecurity domain. Real time log monitoring is one of the best ways to ensure business data security and integrity.

A well suited SIEM implementation ensures the ability to systematically store, create and retrieve the logs for active Monitoring, Analysis and Compliance requirements.

An SIEM brings a wide array of security functionalities that are critical for an organization's IP security. [↗](#)



SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117

[sos@infopercept.com](mailto:sos@infopercept.com)

[www.infopercept.com](http://www.infopercept.com)

