Published on *Tux Machines* (http://www.tuxmachines.org)

Security and Scare for Sale

By *Roy Schestowitz*
Created *23/02/2020 - 5:10pm*
Submitted by Roy Schestowitz on Sunday 23rd of February 2020 05:10:30 PM Filed under Security [1]

- **Malware Attack Takes ISS World's Systems Offline [2]**

  > Founded in 1901, the Copenhagen, Denmark-based company provides cleaning, support, property, catering, security, and facility management services for offices, factories, airports, hospitals, and other locations all around the world.
  >
  > At the moment, the company?s employees don?t have access to corporate systems, as they were taken offline following a malware attack earlier this week.

- **The rise and rise of ransomware [3] [iophk: Windows TCO]**

- **Security flaws belatedly fixed in open source SuiteCRM software [4]**

  > According to Romano, a second-order PHP object injection vulnerability (CVE-2020-8800) in SuiteCRM could be ?exploited to inject arbitrary PHP objects into the application scope, allowing an attacker to perform a variety of attacks, such as executing arbitrary PHP code?.
  >
  > SuiteCRM versions 7.11.11 and below are said to be vulnerable.
  >
  > [...]
  >
  > ?We have put a notice on our open source community channels and advice via social media. We have a dedicated community that works around the clock to spot vulnerabilities and produce suitable fixes, which is one of the key benefits for a business when choosing to use

open source software.?

- **[With the rise of third-party code, zero-trust is key](https://techbeacon.com/security/rise-third-party-code-zero-trust-key) [5]**

  The surface area of website and web application attacks keeps growing. One reason for this is the prevalence of third-party code. When businesses build web apps, they use code from many sources, including both commercial and open-source projects, often created and maintained by both professional and amateur developers.

  Web application creators take advantage of third-party code because it allows them to build their websites and apps quickly. For example, companies are likely to add a third-party chat widget to their site, instead of building one from scratch.

  But third-party code can leave websites vulnerable. Consider the July 2018 Magecart attack on Ticketmaster. In this data breach, hackers were able to gain access to sensitive customer information on Ticketmaster's website by compromising a third-party script used to provide chatbot functionality.

  The challenge is that this third-party functionality runs directly on the customer's browser, and the browser is built to simply render the code sent down from a web server. It assumes that all code, whether first-party or third-party, is good.

- **New company BluBracket takes on software supply chain code security [6]**

- **BluBracket scores $6.5M seed to help secure code in distributed environments [7]**

  BluBracket, a new security startup from the folks who brought you Vera, came out of stealth today and announced a $6.5 million seed investment. Unusual Ventures led the round with participation by Point72 Ventures, SignalFire and Firebolt Ventures.

Security

Source URL: http://www.tuxmachines.org/node/134394

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.securityweek.com/malware-attack-takes-iss-worlds-systems-offline
[3] https://www.axios.com/the-rise-and-rise-of-ransomware-c2f03afc-cd7d-423e-b29a-bcda9572bfac.html
[4] https://portswigger.net/daily-swig/security-flaws-belatedly-fixed-in-open-source-suitecrm-software
[5] https://techbeacon.com/security/rise-third-party-code-zero-trust-key

[6] https://www.zdnet.com/article/new-company-blubracket-takes-on-software-supply-chain-code-security/

[7] https://techcrunch.com/2020/02/19/blubracket-scores-6-5m-seed-to-help-secure-code-in-distributed-environments/