Hello all, and welcome to another week of TWIS! This week, we're covering the ever-so-popular topic of insider shenanigans, love in the digital age, stingy bug bounties, medical data leaks, and another hole for Cisco. Unintentionally, this issue of TWIS leans strongly towards the importance of human diligence and its relation to security - seeing as how the human aspect of security is becoming a more popular target, hopefully this gives perspective!

NVD Showcase

This section lists the topmost CVEs for the past week based on severity score. A link to the CVE and a short summary has been provided.

CVSS	Summary	Severities
CVE-2020-15642	This vulnerability allows remote attackers to execute arbitrary code on affected installations of installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the isHPSmartComponent method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10501.	*V3.1:* 8.8 HIGH *V2.0:* 9.0 HIGH
CVE-2019-4713	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 172084.	V3.1: 8.8 HIGH V2.0: 9.0 HIGH
CVE-2020-5624	SQL injection vulnerability in the XooNIps 3.48 and earlier allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	*V3.1: 9.8 CRITICAL V2.0: 7.5 HIGH*
CVE-2020-4587	IBM Sterling Connect:Direct for UNIX 4.2.0, 4.3.0, 6.0.0, and 6.1.0 is vulnerable to a stack based buffer ovreflow, caused by improper bounds checking. A local attacker could manipulate CD UNIX to obtain root provileges. IBM X-Force ID: 184578.	*V3.1:* 7.8 HIGH *V2.0:* 7.2 HIGH

Patch Tuesday

No Patch Tuesday this week! Stay tuned for next month's patch rundown.

Weekly Article Review

Disgruntled Destruction

In the world of security and business, almost every employee is considered to be both a huge blessing and a considerable liability. With the proper mixture of good technical security measures (like encryption) and excellent policy development and implementation, it is rare that any security incident will have enough ground to stand on in order to cause considerable damage to a business.

Unfortunately, Cisco had a considerable gap in their policy. A disgruntled former employee of Cisco left the company back in late 2018 and, five months after resignation, logged back into his account and deleted a massive amount of accounts and resources. Among the wreckage was over 16,000 WebEx Teams accounts and 456 virtual machines hosting the Cisco WebEx Teams application.

Though this occurred in late 2018, the engineer recently plead guilty to the actions and is scheduled for a hearing come end of December, but not after creating over $2.4 million in damages through Cisco's refunds and lack of service availability.

Digital Love

Online dating is rough. With catfishing, scams, and a considerable amount of ghosting, it's hard to catch a break, but sometimes relationships do blossom through the format.

Unfortunately, abuse of online dating platforms is on the rise. From 2017 to now, 'confidence fraud' and romance scams have grown at an exponential rate, taking the second most popular form of cybercrime just behind Business Email Compromise (BEC). After providing this information, the FBI has warned against jumping headfirst into online dating, providing some tips and tricks to romancing on these platforms:

- Research the person's photo and profile using online searches to see if the material has been used elsewhere.

- Go slow and ask questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to go “offline.”
- Beware if the individual attempts to isolate you from friends and family or requests.
- Beware if the individual promises to meet in person, but then always comes up with an excuse why he or she can’t. If you haven’t met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you don’t know personally.

That isn’t the only mention of online dating given this week. U.S. Democratic campaign staffers were warned against putting out too much information on their online profiles by security officials as concerns of opposition ‘sting’ campaigns rose. The primary concern in these cases is not just money, though, but political image.

Stingy Slacker

Slack caught a huge break when a high-criticality vulnerability was intercepted by a security researcher and reported via HackerOne. The researcher, Oskars Vegeris, was even helpful in providing a long explanation to the issue, a video proof-of-concept, and even a TL;DR (too long;didn’t read) for brevity!

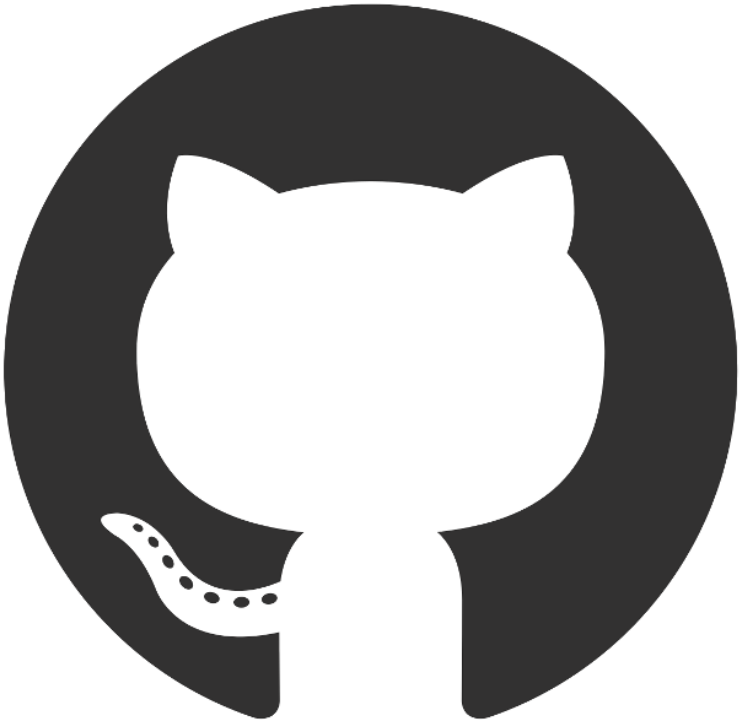
In response, he didn’t receive the praise expected for such a large issue. In fact, a measly collective $1,750 was paid out for his and his collaborator’s efforts, and Slack denied his initial request for disclosure. At the same time as that denial for disclosure, the RCE exploit was published on Slack’s website without mention of Vegeris or his writeups, staying without credit until Vegeris mentioned it.

Needless to say, for the severity of his reports and the importance of Slack as a product for businesses, Vergeris was not paid well and the path that Slack took for publication of the issue was frowned upon by most of the Twitter-verse (though what isn’t?).

Git Checked

Unfortunately, it’s not always malicious intention that causes the mass release of information. In the case of a medical data leak to GitHub, it may be because of misconfigured access controls. Hardcoded login credentials embedded within code, public repositories, and a lack of two-factor authentication all contributed to the easy viewing of HIPAA-protected information.

Dutch security researcher Jelle Ursem explained that the trove of nine companies’ worth of sensitive data was not at all hard to access. In fact, all he did was search a few phrases on GitHub. The exposure went undetected for nine months, but resulted in Ursem publishing a paper on the unfortunate trend of mishandling customer data on GitHub.



Traffic Jam

Have you ever made a mistake that made your heart jump? Rest easy - it can't be as bad as this. If you were surfing the internet this Sunday and had a momentary desire to perform percussive maintenance, you're not alone. A massive CenturyLink outage caused a 3.5% drop in worldwide internet traffic, spreading out from CenturyLink to other ISPs and affecting large websites like Reddit and Hulu (I was at a suspenseful moment in Lovecraft Country!!).

Cloudflare speculates that a series of BGP updates on a Flowspec rule caused the problem. Seeing as how Flowspec, created by Cisco, has the primary purpose of quickly spreading configurations across a network to mitigate possible DDoS attacks, it makes some ironic sense that it would cause a massively spreading unintentional worm throughout CenturyLink's network.

Cisco's Carrier Conundrum

Though this vulnerability may not appear directly harmful like the ones above, it can still cause massive issues with device availability if used correctly. CVE-2020-3566 and CVE-2020-3569 were published with warning by Cisco over the weekend and are unpatched. With proper action from an attacker, these vulnerabilities may cause a remote and unauthenticated user to exhaust all process memory.

The Cisco IOS XR Network OS, deployed on a series of carrier-grade routers, is vulnerable to crafted Internet Group Protocol Management (IGMP) packets. If multicast routing and IGMP are enabled on the router, memory exhaustion may be seen through the system logs. Though no workarounds currently exist, Cisco suggests using a network baseline of IGMP traffic to reduce the amount of IGMP traffic allowed through the router, mitigating possible denial of service.

Tesla Foil

Sometimes, it's just not worth it. An employee at Tesla recently turned down a million-dollar bribe from an old acquaintance to install malware on Tesla's network. Russian national Egor Igorevich

Kriuchkov, a man whom the Tesla employee had met four years prior, contacted the employee via WhatsApp with few details. After meeting in person, Kriuchkov related the details of his plan, including the $250,000 malware build by a Russian hacking group to be used.

The Tesla employee contacted the FBI and Tesla after the first meeting, continuing to record their meetings and even negotiating with Kriuchkov, who was arrested upon attempting to leave the country. He is currently being held in the U.S.

So what does this mean for corporations? As with the story of the Cisco engineer above, it means to keep your eyes open for departing and disgruntled employees. Employees are not a threat, the access that is being provided to them is. If proper exit protocols, a close eye on employee quality-of-life, and monitoring are used, insider events are less likely to occur.

That's about it for now. If you're itching for more information on daily, weekly, and monthly happenings, here's a listing of suggested sources that might tickle your fancy. Got an interesting article you'd like featured? Feel free to toss it over in an email with the header: **This Week In Security** or **TWIS**, and it'll get a review.

Podcasts:
(New to Podcasts? Recommended players are Spotify and PocketCasts)
Cyberwire Daily Podcast
ThreatPost Daily Podcast
Smashing Security (Weekly)
Hacking Humans by Cyberwire (Weekly, social engineering)
Hak5 Podcast (Weekly)
The Social Engineer Podcast (Monthly)
The Shared Security Podcast (Weekly)

Websites:

https://krebsonsecurity.com/
https://threatpost.com/
https://www.darkreading.com/
https://www.wired.com/
https://www.social-engineer.org/
https://thecyberwire.com/
https://news.sophos.com/en-us/
https://www.bleepingcomputer.com/
https://techcrunch.com/