ISSUE
08
December
2020

MONTHLY TECH TIPS TechTalk

this issue

Millions Affected As Gmail, YouTube, GSuite Suffers Outage

Services including Gmail, YouTube, Google Drive and Google Classroom suffered a widespread outage Monday, affecting many users and employers. Reports of the crash spiked around 6:30 a.m. Eastern time, according to DownDetector.

The outage appeared to be related to the authentication tools of the company, which handle how users log in to services run by developers from Google and third-parties.

GSuite Outage Proves Need For Duplication.

On Monday morning, a large percentage of Gmail users worldwide were receiving errors related to authentication and were unable to open email in mail applications or browsers.

The outage impacted people who rely on Google for work, as well as schools who were reporting on social media that their students could not log into their Chromebooks. This is bad timing with all the students who are relying on remote learning during the coronavirus pandemic. One Indianapolis high school said it was delaying classes two hours because of the problem.

Business Impact:

The outage lasted about for about 45 minutes which was enough to send businesses into a panic. Several clients called ASSI wondering why they could not access their services. One of our clients uses a SaaS Backup solution that allowed them to access their GSuite files. How did they accomplish this? That use the Datto SaaS solution which performs several backups of your GSuite or Microsoft 365 data throughout the day, allowing you to revery to an earlier point in time for data access.

Cloud-based backups, of cloud-based data:

Many businesses consider the cloud-based data retention provided from Google and Microsoft to be their data backup, but Microsoft says quite clearly that they are not responsible for restoring your data.

The best option is to use a cloud-based backup solution to ensure that you can access to your data in the event your primary provider goes offline.
Want to review your options? It’s always free to talk technology at ASSI.

Advanced Systems Solutions Inc.

What Is SolarWinds Orion

The SolarWinds Orion Platform offers a single architecture that scales to manage the most complex and geographically dispersed IT environments.

SolarWinds is designed to provide monitoring and management for large enterprise-class infrastructures.

Additional polling engines allow you to scale up to 400,000 elements on a single Orion Platform instance while additional web servers scale the number of supported users. With Enterprise Operations Console (EOC), you can centralize and simplify data management of multiple instances in a single, consolidated view.

The High Availability option helps ensure 24/7 availability for your Orion servers and pollers across subnets.

Source - https://www.solarwinds.com/solutions/orion

SolarWinds Orion Products Exploited

CISA Issues Emergency Directive To Mitigate The Compromise Of SolarWinds Orion Network Management Products.

SolarWinds Orion products (*versions are 2019.4 through 2020.2.1 HF1*) are currently being exploited by malicious actors.
The U.S. Treasury and Commerce Departments were reportedly compromised by a supply chain attack by using SolarWinds Orion.

Statement from SolarWinds

“We have been made aware of a cyberattack to our systems that inserted a vulnerability within our SolarWinds® Orion® versions 2019.4 HF 5, 2020.2 with no hotfix, and 2020.2 HF 1 only. We have been advised that this incident was likely the result of a highly sophisticated, targeted, and manual supply chain attack by an outside nation state, but we have not independently verified the identity of the attacker.”

Required Actions

CISA advises that affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network. Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, agencies are prohibited from (re)joining the Windows host OS to the enterprise domain. Affected entities should expect further communications from CISA and await guidance before rebuilding from trusted sources utilizing the latest version of the product available.
Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed.

Apply updates

SolarWinds is asking customers to upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure the security of your environment. This version is currently available at customerportal.solarwinds.com.

If you aren’t sure which version of the Orion Platform products you are using, see directions on how to check that here. To check which hotfix updates you have applied, please go here.

Most importantly, change ALL passwords on the network if you were using the affected versions. This includes all endpoint passwords and passwords for accounts with elevated privileges.

Details Here:

https://bit.ly/SolarWindsBreach

Areas for Review This Month

We recommend that you take this month to review and update policies.

Update fatigue is a real thing. Performing updates is never a fun task, but it is critical and is an effective way to strengthen your security posture.

One area of updates that is often overlooked are the policies and procedures for an organization.

Many organizations were forced to update their procedures when team members were working remotely earlier this year.

Over time, the procedures for specific processes change slightly. One great reason to review is that software updates often change options within the software. When these changes occur, the procedures cannot be easily followed by a new team member.

End of Year

This is a perfect time to review your organizations security policies.

Passwords

Remind your Team Members to change their passwords. Even better, follow NIST standards and implement an automatic password change policy. This will ensure that passwords are changed regularly and are complex.

Security Awareness Training

The biggest weakness on the computer is the human, so we need to secure the human! The easiest way to accomplish this task is to review your security awareness training. Schedule time during team meetings to review key points about security. Keeping IT security as part of your conversations will keep team members alert for any suspicious emails or websites. Even better, take your training to the next level by implementing an email spoofing test to see what team members will take the bait. Let us know if you would like talk about security awareness program, it is always free to talk!

This Month's Q&A Technology Tips

Q: Cole from Cleveland asks, "Should I remove old versions of software or is it better to leave them installed?"

A: Awesome question Cole, thanks for asking!

While it is not imperative to remove versions of software, they can become security vulnerabilities. This happens when a vulnerability is discovered in an old version, and the new version is not downloaded to replace the weaker version.

Some software updates automatically, while other solutions require a manual check and download. This is a great reason to have a solution that checks your entire computer for all updates, not just the operating system.

Many organizations use software solutions that check all attached hardware and installed software to see if there are more recent updates available. This helps to save time from performing a manual inventory of what solutions are in place, and which are out of date. Before you remove any software, make sure you have the software keys on hand in case you ever want to reinstall.

Thanks again for the question Cole, I hope this helps!

Have a question?

Ask us at - info@advancedsystemssolutions.com

EYE ON IT

The Hot Trend of December

Adobe Flash Player will no longer be supported after December 2020. The decision to end support for Flash Player was made by Adobe due to the diminished usage of the technology and the availability of better, more secure options such as HTML5, WebGL, and WebAssembly.

After December 2020, you will no longer receive security updates for Adobe Flash Player from Microsoft. Beginning in January 2021, Adobe Flash Player will be disabled by default and all versions older than June 2020 will be blocked.

The vulnerability us is actually within the browser, not in Flash itself. That is the point where potential attackers can exploit vulnerabilities and plant malware.

None-the-less, network administrators should plan to remove Adobe Flash from endpoints within the network.

Stay Up to Date!

Don’t forget to check out our additional tips to keep you secure! If you are not familiar with the new features in Edge, you will want to check out our guidelines for keeping your organization secure.

https://bit.ly/ASSI_Blog

Upcoming Events

- ### FLGISA 2021 WINTER SYMPOSIUM

  We are excited that the FLGISA is hosting the 2021 Winter Symposium at the Embassy Suites Lake Buena Vista South in Kissimmee, Florida on January 26-28, 2021. The symposium is open to all Florida local government agency technology professionals. We look forward to seeing you there!

  https://www.flgisa.org/events/

- ### T2 Tech Talk Podcast

  We know tech and marketing can be daunting, but we break it down into byte sized chunks.

  https://www.t2techtalkpodcast.com/

- ### Orlando Power Lunch

  The Orlando Power Lunch is a virtual luncheon that provides networking as well as tips from informative speakers. You won’t want to miss these events!

  https://www.orlandopowerlunch.com

Advanced Systems Solutions Inc.

1051 Winderley Place #307
Maitland, FL 32751
407-414-6626
www.advancedsystemssolutions.com