OCISO DIR
OFFICE OF THE
CHIEF INFORMATION SECURITY OFFICER
STATE OF TEXAS

Texas Cybersecurity Weekly

Collected news & information for Texas' cybersecurity community

TLP:WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

Assistance/Feedback/Questions?

Email the Office of the CISO at
DIRSecurity@dir.texas.gov

The periodical aggregates information about cybersecurity and information technology to promote shared awareness, cyber hygiene, and information sharing amongst government, the private sector, and all Texans.

News and Commentaries

Discouraging the Use of Guest Accounts

Use of guest accounts and other generically named or shared accounts should be avoided as an enterprise best practice.

Guest accounts anonymize the individual using the system. Because the user is utilizing a guest account, all the actions are initiated as that guest account, and recorded as such in any logs. To track down who the responsible individual is, a review of who was sitting at the machine or connecting to it remotely has to be manually initiated. It also adds a level of plausible deniability for the attackers, since they can claim that someone else was sharing the access with them. This lack of accountability generally represents an unacceptable risk and should be avoided in favor of explicitly named accounts, usually following an established naming convention.

Guest accounts are rarely as secure as most people believe. By allowing guest accounts, a dedicated attacker now has a foot in the door to your systems. While guest modes typically don't allow the installation of software, most do allow the user to surf the web, where they can easily access nefarious web sites that have software designed to bypass the basic security settings that guest accounts have. Some guest accounts also allow the opening of various file types that can have malware, or allow attackers to perform intel gathering on your infrastructure that they can then exploit in a subsequent attack.

Due to the risks posed, use of guest and generically named accounts should be avoided except for very limited use cases where anonymity is a critical component of the business process being performed. For more information on proper account management, reference NIST 800-53 revision 4, controls AC-2 and IA-4.
NIST link - https://nvd.nist.gov/800-53

Vigilante Hackers

Vigilante hackers exploited a vulnerability in Cisco Smart Install Client to target critical infrastructure, leaving American flags and messages on machines in both Russia and Iran.

https://motherboard.vice.com/en_us/article/a3yn38/election-hacking-vigilante-russia-iran-cisco

Unpatched Vulnerabilities the Source of Most Data Breaches

Organizations in a new Ponemon Institute study say they were hit with one or more data breaches in the past two years, and 34% say they knew their systems were vulnerable prior to the attack. The study surveyed nearly 3,000 IT professionals worldwide on their patching practices. https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

Annual Industry Reports

Verizon 2018 Data Breach Investigations Report

2,216 confirmed data breaches.

What went wrong? An exploration in trends and data.

Within the 53,000+ incidents and 2,200-odd breaches you'll find real takeaways on what not to do, or at the very least, what to watch for.

Verizon released their annual report available at https://www.verizonenterprise.com/verizon-insights-lab/dbir/

NetDiligence 2018 Cyber Claims Study

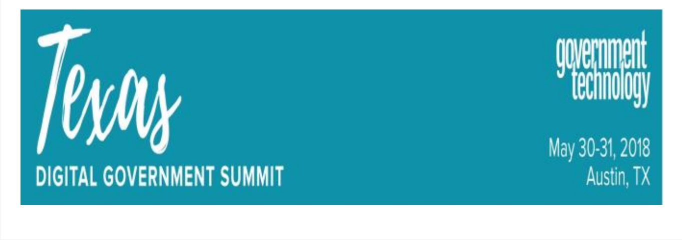
The annual NetDiligence® Cyber Claims Study uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer's perspective.

NetDiligence released their annual report available at https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition-1.3.pdf

Workforce Development and Events

The 18th annual Information Security Forum will be held May 23-24, 2018 at the Palmer Events Center in Austin, Texas, and is hosted by the Texas Department of Information Resources (DIR) and managed by the Office of the Chief Information Security Officer (OCISO).

http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=140



Government Technology's passion is helping spread best practices and spurring innovation in the public sector. The Texas Digital Government Summit is designed to do just that. The summit has an advisory board that gathers public and private sector leaders to create an agenda designed to make that passion relevant and actionable to the state and local government organizations attending the summit.
http://www.govtech.com/events/Texas-Digital-Government-Summit.html

Texas Government Data Forum 2018

Thursday, June 21, 2018 | 8:00 am - 4:30 pm | Austin, TX

Annual conference hosted by the Texas Department of Information Resources. Any government/public sector employees may attend.
http://dir.texas.gov/View-About-DIR/Calendar-Detail.aspx?id=456&month=6&year=2018&type=list#detail

Vulnerability Alerts

Adobe Releases Security Updates
Original release dated: April 10, 2018

Adobe has released security updates to address vulnerabilities in Adobe PhoneGap Push Plugin, Adobe Digital Editions, Adobe InDesign, Adobe Experience Manager, and Adobe Flash Player. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. NCCIC encourages users and administrators to review Adobe Security Bulletins APSB18-15, APSB18-13, APSB18-11, APSB18-10, and APSB18-08, and apply the necessary updates.

Microsoft Releases April 2018 Security Updates

Original release date: April 10, 2018

Microsoft has released updates to address vulnerabilities in Microsoft software. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.
NCCIC encourages users and administrators to review Microsoft's April 2018 Security Update Summary and Deployment Information and apply the necessary updates.

Multiple Vulnerabilities in Cisco IOS, IOS XE and IOS XR Could Allow for Remote Code Execution

MS-ISAC Advisory Number: 2018-034 - UPDATED
Date: 03/28/2018; 04/09/2018 - UPDATED

There are reports of the vulnerability CVE-2018-0171 being exploited in the wild successfully by hacktivist botnets in a campaign against Iran. Cisco is also aware of a significant increase in Internet scans attempting to exploit instances where the Smart Install feature is enabled and not secured. It is important to note that both attacks require a Cisco device to be running a vulnerable version of the Smart Install feature on open port 4786.

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-ios-ios-xe-and-ios-xr-could-allow-for-remote-code-execution_2018-034/

Multiple Vulnerabilities in Adobe ColdFusion Could Allow for Remote Code Execution (APSB18-14)

MS-ISAC Advisory Number: 2018-038
Date Issued: 04/10/2018

Multiple vulnerabilities have been discovered in Adobe ColdFusion, the most severe of which could allow for remote code execution. Adobe ColdFusion is a web application development platform. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

https://helpx.adobe.com/security/products/coldfusion/apsb18-14.html

Critical Patches Issued for Microsoft Products, April 10, 2018

MS-ISAC Advisory Number: 2018-040
Date Issued 04/10/2018

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

A full list of all vulnerabilities can be found at the link below:
https://portal.msrc.microsoft.com/en-us/security-guidance/summary

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution (APSB18-08)

MS-ISAC Advisory Number: 2018-039

Date Issued: 04/10/2018

Multiple vulnerabilities have been discovered in Adobe Flash Player, the most severe of which could allow for remote code execution. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation of the most severe of these vulnerabilities could result in the attacker gaining control of the affected system. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

https://helpx.adobe.com/security/products/flash-player/apsb18-08.html

Breach Events

Best Buy Suffers Customer Payment Data Breach

A third party used by Best Buy to provide online chat services suffered a cyber intrusion.

https://www.pcmag.com/news/360306/best-buy-suffers-customer-payment-data-breach

Delta Air Lines and others Hit by Data Breach

On March 28, Delta was notified by [24]7.aiopens, a company that provides online chat services for Delta and many other companies, that [24]7.ai had experienced a cyber incident. Among others, both K-Mart and Sears were impacted as well.

Delta Updates:
https://www.bizjournals.com/southflorida/news/2018/04/09/delta-air-lines-hit-by-data-breach.html
Sears and K-Mart
https://www.cnet.com/news/delta-sears-kmart-data-breach-credit-card-address/