FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter **March 7, 2016**

Newsletter Contents

FS-ISAC Webinars

Getting Rid of Passwords for Good - Challenges and Alternatives
Transmit Security | March 29
Register here

White Paper: Cybercrime Report Q4 2015
ThreatMetrix | Available until April 1
Register here

Webinar
BrandProtect | April 13
Additional Information to Follow

Upcoming Events

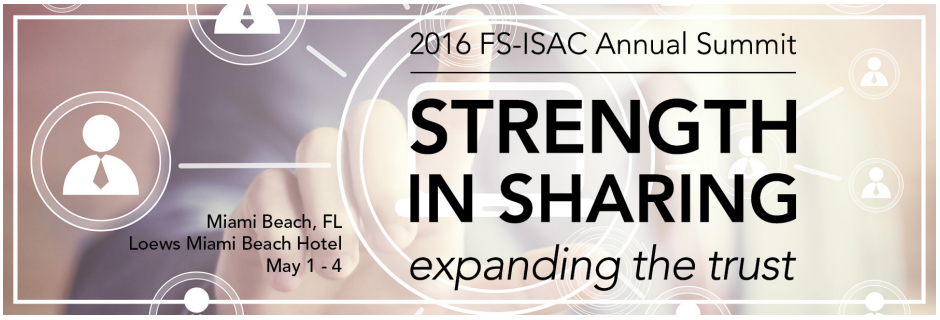
Cyber Threat Intelligence Training
Reston, VA | March 14 - 17
Register here

Information Sharing Workshop: "Security Analytics"
Chicago, IL | April 5
Register here

Information Sharing Workshop
Amsterdam, Netherlands | April13
Register here

2016 FS-ISAC Annual Summit
Miami Beach, FL | May 1 - 4
Register here

2016 FS-ISAC APAC Summit
Singapore | June 20-22
Register here



Early Bird Registration Ends April 1

The FS-ISAC Annual Summit is just around the corner. Make sure to register today as Early Bird Registration ends April 1; then book your room for the beautiful Loews Miami Beach Hotel, May 1-4. This year's summit will explore "Strength in Sharing" through expert-led panels, forums, and break-out sessions. Visit www.fsisac-summit.com for more information.

APAC Summit - Singapore

FS-ISAC will be hosting the first APAC Summit this June 20-22 in Singapore. Registration is open, so be sure to take advantage of the Early Bird period – now through May 20! Visit www.fsisac-summit.com/2016-apac-summit for more details.

Save the Date: Fall and European Summits

This year's Fall Summit will be held October 23-26 at the Gaylord Opryland in Nashville, TN. Visit www.fsisac-summit.com/2016-fall-summit for more details, and stay tuned for registration and updates.

The European Summit will bring us to Barcelona, Spain, November 7-8. Keep your eye on www.fsisac-summit.com for updates and registration. You will not want to miss this Summit.

CISA Implementation

The Department of Homeland Security (DHS) and the Department of Justice (DOJ) issued guidance to assist private entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Act of 2015, which the US Congress passed and the President signed in December 2015. Highlights of the release include:

- Identifying personally identifiable information (PII) and how to scrub it from a cyber threat indictor
- Indicating possible consequences for the inclusion of PII in information shared with the government
- Providing methods for sharing indicators and defensive measures
- Providing an outline of liability protections granted by CISA

FS-ISAC recently participated in a Financial Services Roundtable media event to discuss implementation of the Cybersecurity Act along with senior staff from key members of Congress, and senior officials from the US Departments of Homeland Security, Justice, and Treasury.

continued on next page

Membership Call Recording

ICYMI - The Member Update Call from February is now available on the Portal. Hear from President and CEO Bill Nelson and others as they discuss the rapid growth of FS-ISAC membership, new initiatives, global expansion, and more. The recording is located under the "Documents" section of the Portal in "FS-ISAC Webinars" folder. Please note the audio starts about 45 seconds into the presentation.

From the FS-ISAC Analysis Team

Vulnerability in GNU C Library - CVE-2015-7547

A vulnerability in GNU's C Library (glibc) could be exploited to cause system crashes or remote code execution on systems utilizing the vulnerable library. Glibc is the GNU Project's implementation of the C standard library, and is designed to be a portable and high performance C library. The part of glibc that handles DNS lookups is vulnerable to a buffer overflow that can lead to denial of service or remote code execution on the affected host.

An attacker can get an affected client to look up a malicious domain and return a payload that exploits this vulnerability. If the code is being run as root or sudo, then it can potentially lead to a crash, or complete compromise of the server/system. The remote code execution exploit is reported (by Google) to provide the attacker with complete control over the EIP (extended instruction pointer) register.

The FS-ISAC Analysis Team is not currently aware of any exploit activity. However, a researcher named Fermin Serna posted a Github repository claiming to be working on a proof-of-concept code.

Risk to Financial Institutions

The vulnerability can be a jumping off point in which malicious actors will develop an evil exploit, including potentially remote code execution. Remote code execution allows an attacker to take over the vulnerable process.

- It is possible for malicious actors to write correctly formed DNS responses with attacker-controlled payloads that will penetrate a DNS cache hierarchy, and therefore allow attackers to exploit machines behind such caches
- The impact of a such cyber-event can result in civil, financial, legal, regulatory, and reputational issues that may impede an institution's ability to remain in operation.

Remediation

Financial institutions and their service providers should assess the risk to their infrastructures and execute mitigation activities with appropriate urgency. Financial institutions should identify all servers, systems, and appliances that use the vulnerable versions of Bash and follow appropriate patch management practices. Financial institutions relying on third-party service providers should ensure those providers are aware of the vulnerability and are taking appropriate mitigation action.

Institutions are encouraged to patch vulnerable systems, especially internet-facing systems, **as soon as possible**:

1. Upgrade affected operating systems to patched versions
2. Upgrade applications using vulnerable versions of Glibc to patched versions
3. Upgrade any other installations of Glibc to patched versions
4. Recompile in-house applications that are compiled with static links to Glibc
5. If a device cannot be patched in a timely manner, consider removing the web-facing device, if practical. Otherwise, consider adding extra monitoring of the device until patches can be applied.