Threat Alert Level is remaining at Blue (Guarded), as per the last evaluation on June 5, 2019. This is due to multiple vulnerabilities in Google Android OS and Chrome.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

21 June 2019

In The News This Week

Tap 'n Ghost Attack Let Hackers to Remotely Control Android Smartphones.

A new attack dubbed Tap 'n Ghost are targeting Near Field Communication (NFC) enabled Android smartphones and let attackers trigger malicious events on the victim's smartphone and even take control over the smartphone remotely. Nowadays, smartphones are used to interact with several networking devices that include wireless headphones, fitness devices, contactless payment systems, and other devices. To connect with the networking devices smartphones are shipped with a number of cellular networks such as Wi-Fi, Bluetooth, and NFC. The new attack leverages the Near Field Communication (NFC) implementation of the Android OS version 4.1 or later.

After a survey with 300 respondents and a user study involving 16 participants, researches from Waseda University found the Tap 'n Ghost attacks are realistic and totally exploitable.

Tap 'n Ghost Attack Techniques - With Tap 'n Ghost, researchers derived two attack techniques which let hackers trigger malicious events on the victim's Android smartphone. (1) Tag-based Adaptive Ploy (TAP): TAP attack works with a web server, it makes use of device fingerprinting and comprises of a NFC tag emulator using a single board computer with a Wi-Fi controller installed (Like a Raspberry Pi). Once the victim's phone comes near to the emulator, it reads the tag and launches the browser to open the malicious URL recorded in the NFC tag and the website employs device fingerprinting of the victim device and based on this information, the single board computer determines the tag suited for the victim's device. TAP can perform a tailored attack on the victim's smartphone, for example; popping up a customized dialog box asking whether or not to connect to an attacker's Bluetooth mouse." (2) Ghost Touch Generator: This attack relies on scattering the events around the original touch area, even if the victim wants to touch a cancel button to disconnect from a malicious Wi-Fi, the attacker can make the system switch the touch to "connect" rather than "cancel". Read the full story here:

Vulnerability Report – FireFox Users

Emergency!! Zero-day Flaw in FireFox Let Hackers Take Full Control of Your Computer

Update Your FireFox Now!

Reported on **18 June 2019** - CVE-2019-11707: Type confusion in "Array.pop"

All versions prior to Firefox 67.0.3 and Firefox ESR 60.7.1 are vulnerable.

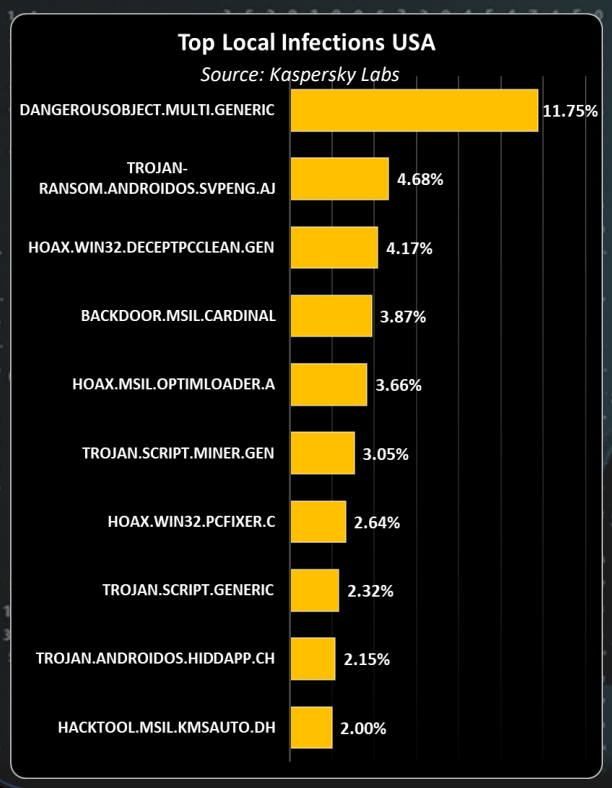
Description: A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in "Array.pop". This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw.

A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals.

How to update Firefox to the latest release:

1. Click the menu button ☰ in the top right corner , click "Help" and select "About Firefox".
2. The "About Mozilla Firefox" window will open, and Firefox will begin checking for updates and download and install them automatically. (progress will be shown in the dialog box)
3. When the download is complete, click "Restart" to update Firefox.

Reference: Mozilla & GBHackers



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

According to Symantec

There are around **24,000** malicious mobile apps blocked every day

OWASP Top 10 Proactive Controls – What is it?

Having a Web APP developed? Ask the developer if it is done according to the OWASP framework

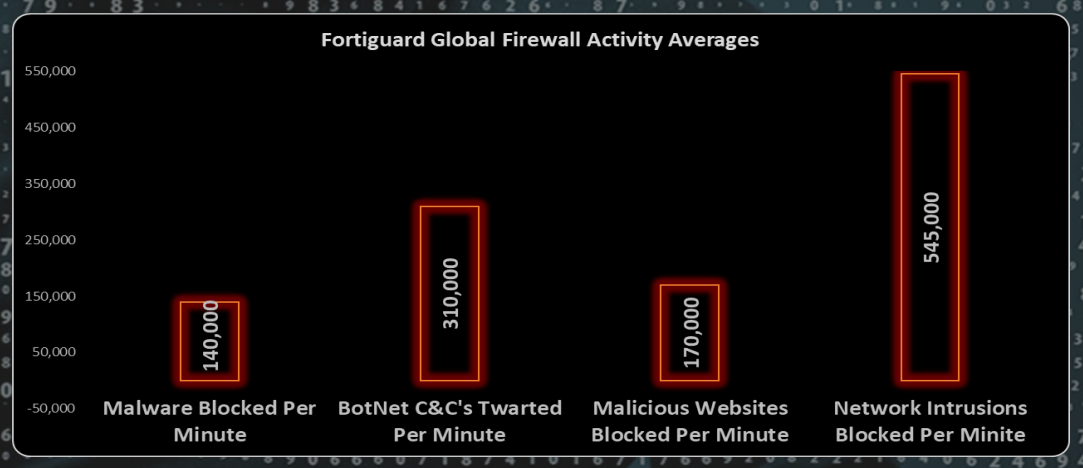
The Open Web Application Security Project (OWASP) is a non-profit educational charity dedicated to enabling organizations to design, develop, acquire, operate, and maintain secure software. All OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. In this bulletin today, we will explore a summary of the top 10 proactive controls proposed by OWASP. The OWASP Proactive Controls document is free to use under the Creative Commons ShareAlike 3 License.

Software developers are the foundation of any application. In order to achieve secure software, developers must be supported and helped by the organization they author code for. As software developers author the code that makes up a web application, they need to embrace and practice a wide variety of secure coding techniques. All tiers of a web application, the user interface, the business logic, the controller, the database code and more – all need to be developed with security in mind.

The following section highlights the 10 controls with description summaries, for full details please refer to the OWASP proactive controls document.

(1) Define Security Requirements - A security requirement is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied. Those same vetted security requirements provide solutions for security issues that have occurred in the past. Requirements exist to prevent the repeat of past security failures. (2) Leverage Security Frameworks and Libraries - Secure coding libraries and software frameworks with embedded security help software developers guard against security-related design and implementation flaws. A developer writing an application from scratch might not have sufficient knowledge, time, or budget to properly implement or maintain security features. Leveraging security frameworks helps accomplish security goals more efficiently and accurately. (3) Secure Database Access - This section describes secure access to all data stores, including both relational databases and NoSQL databases. The areas to consider: Secure queries, Secure configuration, Secure authentication and Secure communication. (4) Encode and Escape Data - Encoding and escaping are defensive techniques meant to stop injection attacks. Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the "<" character into the < string when writing to an HTML page. Escaping involves adding a special character before the character/string to avoid it being misinterpreted, for example, adding a "\" character before a "" (double quote) character so that it is interpreted as text and not as closing a string. (Full description in OWASP) (5) Validate All Inputs - Input validation is a programming technique that ensures only properly formatted data may enter a software system component. (6) Implement Digital Identity - Digital Identity is the unique representation of a user (or other subject) as they engage in an online transaction. Authentication is the process of verifying that an individual or entity is who they claim to be. Session management is a process by which a server maintains the state of the user's authentication so that the user may continue to use the system without re-authenticating. (7) Enforce Access Controls - Access Control (or Authorization) is the process of granting or denying specific requests from a user, program, or process. Access control also involves the act of granting and revoking those privileges. It should be noted that authorization (verifying access to specific features or resources) is not equivalent to authentication (verifying identity). There are several different types of access control design that should be considered. Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) (8) Protect Data Everywhere - Sensitive data such as passwords, credit card numbers, health records, personal information and business secrets require extra protection, particularly if that data falls under privacy laws (EU's General Data Protection Regulation GDPR), financial data protection rules such as PCI Data Security Standard (PCI DSS) or other regulations. (9) Implement Security Logging and Monitoring - Logging is a concept that most developers already use for debugging and diagnostic purposes. Security logging is an equally basic concept: to log security information during the runtime operation of an application. Monitoring is the live review of application and security logs using various forms of automation. (10) Handle All Errors and Exceptions – Exception handling is a programming concept that allows an application to respond to different error states (like network down, or database connection failed, etc) in various ways. Handling exceptions and errors correctly is critical to making your code reliable and secure. Error handling is also important from an intrusion detection perspective. Certain attacks against your application may trigger errors which can help detect attacks in progress.

Adapted from the OWASP Top 10 Proactive Controls document which you can find here: https://www.owasp.org/



Author: Chris Bester
chris.bester@yahoo.com