certTonga

Tonga National Computer Emergency Response Team

Ministry of Meteorology Energy Information
Disaster Management Environment
Climate Change and Communications

TLP: White[1]

Security Bulletin – August 2019

Dear Constituents,

As for the cyber security has increased, the threats and the risk on on High Alert. This is a security alert in advising our people in making sure that they stay alert on the cyber threats and how to mitigate such risks.

Vulnerabilities with Active Exploits in the Wild

Adobe ColdFusion Arbitrary Command Injection Vulnerability *(CVE-2019-7839)*

Multiple vulnerabilities have been discovered in Adobe ColdFusion, the most severe of which could allow for arbitrary code execution. Adobe ColdFusion is a web application development platform. Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application.

How it works

The file extension blacklist bypass, command injection, and deserialization of untrusted data error could all lead to arbitrary code execution if left unresolved.

What to do

- Coldfusion 2018- Updated version 4
- Coldfusion 2016- Updated version 11
- Coldfusion 11- Updated version 19

Reference

Adobe: https://helpx.adobe.com/security/products/coldfusion/apsb19-27.html

D-Link DSL-2750U Multiple Authentication Bypass Vulnerabilities *(CVE-2019-1010155)*

D-Link DSL-2750U is exposed to multiple authentication bypass vulnerabilities.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

An attacker can exploit these issues to bypass authentication mechanism and perform unauthorized actions. This may lead to further attacks.

What to do

Users who has D-Link devices check the D-Link Support website regularly for updates.

Reference

Security Focus- https://www.securityfocus.com/bid/109351

Joomla Remote code Execution Vulnerability *(CVE-2019-14654)*

Joomla has been prone to a security vulnerability by filtering attributes in subform fields allows remote code execution.

How it works

In Joomla, inadequate filtering allows users authorised to create custom fields to manipulate the filtering options and inject an unvalidated option.

What to do

Upgrade to Joomla! version 2.5.14 / 3.1.5 or later.

Reference

Joomla- https://developer.joomla.org/security-centre/787-20190701-core-filter-attribute-in-subform-fields-allows-remote-code-execution.html

Microsoft Windows Kernel Information Disclosure Vulnerability *(CVE-2019-1125)*

An information disclosure vulnerability exists when certain central processing units speculatively access memory. An attacker who successfully exploited the vulnerability could read privileged data across trust boundaries.

How it works

To exploit this vulnerability, an attacker must log on to an affected system and run a specially developed application. The vulnerability would not allow an attacker to directly increase user privileges. But the vulnerability could be used to obtain information that could be used to attempt to further compromise the affected system.

What to do

Users who have Windows Update enabled and have applied the security updates released on July 9, 2019 are protected automatically. This vulnerability does not require a microcode update from your device manufacturer

Reference

Microsoft - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1125

Microsoft Remote Desktop Services Remote Code Execution Vulnerability

(This CVE ID is unique from CVE-2019-1181, CVE-2019-1182, CVE-2019-1222)

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. To exploit the vulnerabilities, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

Please do refer to our advisory to read more
https://www.cert.gov.to/wp-content/uploads/2019/08/Microsoft-August-2019-Patch-Tuesday.pdf

Adobe Security Update for Adobe Acrobat and Reader (CVE-2019-8045)

Adobe Acrobat and Reader versions have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. An attacker could exploit this vulnerability to compromise Confidentiality, Integrity and/or Availability.

Please do refer to our advisory to read more https://www.cert.gov.to/wp-content/uploads/2019/08/Adobe-August-2019-Patch-Tuesday.pdf

Webmin Remote Code Execution Vulnerability (CVE-2019-15107)

Webmin is a web-based interface for system administration for Unix,although recent versions can also be installed and run on Windows.

How it works

Webmin contains a vulnerability that allows remote command execution.The parameter &quot;old&quot; in password_change.cgi contains a command injection vulnerability.

The bug at issue is a pre-authentication command-injection flaw in the &unix_crypt function* used in the password_change.cgi file, used to check the password against the system's /etc/shadow file. By adding a pipe command ("|"), an attacker can execute remote code

What to do

User and System Administrators are strongly recommended to update to the latest version Webmin to 1.930

Reference

Webmin: http://www.webmin.com/security.html

Wordpress Plugin Remote code Execution Vulnerability *(CVE-2019-15092)*

Wordpress Plugin is exposed to CSV injection vulnerability. This allows any application user to inject commands as part of the fields of his profile and these commands are executed when a user with greater privilege exports the data in CSV and opens that file on his machine.

How it works

The webtoffee "WordPress Users & WooCommerce Customers Import Export" plugin 1.3.0 for WordPress allows CSV injection in the user_url, display_name, first_name, and last_name columns in an exported CSV file created by the WF_CustomerImpExpCsv_Exporter class.

What to do

For those who are using Wordpress please do make sure that you update version of plugin to the latest version fixed in 1.3.2

Reference

Plugin Vulnerabilities: https://www.pluginvulnerabilities.com/2019/04/23/our-proactive-monitoring-caught-an-arbitrary-file-upload-vulnerability-in-woocommerce-checkout-manager/

Squid Buffer Overflow Vulnerability *(CVE-2019-12527)*

Squid is exposed to a heap based buffer overflow vulnerability because the application fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.When checking Basic Authentication with HttpHeader, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length is not greater than the buffer, leading to a heap-based buffer overflow with user controlled data. Successfully exploiting this issue allow attackers to execute arbitrary code in the context of the affected application

How it works

When checking Basic Authentication with HttpHeader::getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data

What to do

Users to make sure to update version of squid to the latest version Squid 4.8

Reference

Squid-http://www.squid-cache.org/Advisories/SQUID-2019_5.txt

Other Vulneabilities with known exploits

Misp Cross Site Scripting Vulnerability *(CVE-2019-14286)*

In app/webroot/js/event-graph.js in MISP, a stored XSS vulnerability exists in the event-graph view when a user toggles the event graph view. A malicious MISP event must be crafted in order to trigger the vulnerability.

Palo Alto Networks PAN-OS Multiple Remote Code Execution Vulnerabilities *(CVE-2019-1579)*

Palo Alto Networks PAN-OS is prone to multiple remote code-execution vulnerabilities. Successfully exploiting these issues may result in the execution of arbitrary code in the context of the affected application. Remote Code Execution may allow an unauthenticated remote attacker to execute arbitrary code.

Jenkins Credentials Binding Plugin Information Disclosure Vulnerability *(CVE-2019-1010241)*

Jenkins Credentials Binding plugin is exposed to an information disclosure vulnerability. An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks. Jenkins Credentials Binding Plugin is affected for storing passwords in a recoverable format. Authenticated users can recover credentials.

Apple MacOS Information Disclosure Vulnerability *(CVE-2019-8605)*

A remote attacker could exploit this vulnerability to cause disclosure of information, unauthorized modification and arbitrary code execution with system privileges. A malicious application may be able to execute arbitrary code with system privileges," reads the advisory published by Apple.

Multiple CPU Hardware Information Disclosure Vulnerability *(CVE-2017-5715)*

Multiple CPU Hardware are exposed to an information disclosure vulnerability. Attackers can exploit this issue to obtain sensitive information that may aid in further attacks. Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side channel analysis.

musl libc x87 Stack Overflow Vulnerability *(CVE-2019-14697)*

musl libc has an x87 floating-point stack adjustment imbalance, related to the math/i386/ directory. In some cases, use of this library could introduce out-of-bounds writes that are not present in an application's source code. This can lead to x87 stack overflow in the execution of subsequent math code,

YouPHPTube SQL Injection Vulnerability *(CVE-2019-14430)*

The parameters "User" as well as "pass" of the user registration function in YouPHPTube are vulnerable to SQL injection vulnerabilities. By submitting an HTTP POST request to the URL "/objects/userCreate.json.php" an attacker can access the database and read the hashed credentials of an administrator. Successful exploitation allows an unauthenticated, remote attacker to manipulate SQL queries by injecting arbitrary SQL code or further exploit latent vulnerabilities in the underlying database.

Kubernetes Denial of Service Vulnerability *(CVE-2019-9512,CVE-2019-9514)*

A security issue has been found in the net/http library of the Go language that affects all versions and all components of Kubernetes. The vulnerabilities can result in a DoS against any process with an HTTP or

HTTPS listener. These vulnerabilities allow untrusted clients to allocate an unlimited amount of memory, until the server crashes leading to Denial of Service.

Other Vulnerabilities

- **New coverage available for Godlua malware**

Attackers recently targeted Linux and Windows machines with respective versions of the Godlua malware. The backdoor secures its communication via DNS over HTTPS. The attackers primarily use Godlua as a distributed denial-of-service bot, even launching an HTTP flood attack against one domain

- **Pulse Secure Arbitrary File Disclosure Vulnerability**

Pulse Connect Secure is exposed to arbitrary file disclosure vulnerability. An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, or can send a specially crafted URI to perform an arbitrary file reading vulnerability .

- **New protection rolled out for Microsoft vulnerability exploited in the wild**

The OceanLotus APT recently launched a new malware known as "Ratsnif," which comes in four different variant forms. These rules fire when Ratsnif attempts to make an outbound connection to a command and control (C2) server, or if the malware attempts to download any files. Ratsnif remained undetected after its C2 went online back in August 2018, though researchers believe it's low level of infection kept it under the radar.

- **VMware vulnerability leads to other flaws in NVIDIA Windows GPU display driver**

VMware ESXi, Workstation and Fusion are affected by an out-of-bounds read vulnerability that can be triggered using a specially crafted shader file. This vulnerability can be triggered from a VMware guest, affecting the VMware host, leading to a crash (denial-of-service) of the vmware-vmx.exe process on the host. However, when the host/guest systems are using an NVIDIA graphics card, the VMware denial-of-service can be turned into a code execution vulnerability (leading to a VM escape), because of an additional security issue present in NVIDIA's Windows GPU Display Driver.

- **Palo Alto Network's GlobalProtect Secure Socket Layer (SSL) virtual private network contains remote code execution bug**

CVE-2019-1579 is a remote code execution vulnerability in Palo Alto Network's GlobalProtect Secure Socket Layer (SSL) virtual private network (VPN). At the time of discovery, some systems belonging to ride-sharing service Uber were still at risk, though they have since patched the issue. An attacker could exploit this bug to carry out a buffer overflow, and then gain the ability to remotely execute code on the victim machine.

- **EOS Camera Picture Transfer Protocol Memory Corruption Vulnerability**

A Buffer overflow vulnerability exist in PTP (Picture Transfer Protocol) of EOS series digital cameras that allows an attacker on the same network segment to trigger the affected product being unresponsive or to execute arbitrary code on the affected product via SendObjectInfo command.

- **Fortinet FortiOS Authorization Bypass Vulnerability**

An Improper Authorization vulnerability in Fortinet FortiOS under SSL VPN web portal allows an unauthenticated attacker to modify the password of an SSL VPN web portal user via specially crafted HTTP requests. An attacker can exploit this issue to bypass certain security restrictions and perform unauthorized actions; this may aid in launching further attacks

- **Nimble Streamer Directory Traversal Vulnerability**

Nimble Streamer is exposed to a "../"" directory traversal vulnerability. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of the restricted directory on the remote server.

- **Exim Local Privilege Escalation Vulnerability**

Exim is affected by remote command execution vulnerability. The vulnerability is exploitable instantly by a local attacker, remotely exploit this vulnerability in the default configuration, an attacker must keep a connection to the vulnerable server open for 7 days (by transmitting one byte every few minutes), faster methods may exist. Improper validation of recipient address in deliver_message() function in /src/deliver.c may lead to remote command execution.

Compiled with information from SANS' @RISK: The Concensus Security Vulnerability Alerts

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to

Disclaimer Notice:
The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services