Advisory Alert

Alert No: AAA190417 **Date: 17-Apr-19 14:11 PM**

Classification **The Alert : Public Circulation Permitted**

Security Updates for 17th April 2019

Overview	High	Apache Tomcat VPN	▪ Remote Code Execution Vulnerability ▪ Insecure Cookie management
	Low	Joomla	▪ Directory Traversal
	Informational	WAP3 Microsoft Support Agent Hacked	▪ Protocol Vulnerability ▪ Limited Information Disclosure

Description / Impact

Apache Tomcat

- Apache Software Foundation has released a security update addressing a vulnerability Windows Apache Tomcat. The vulnerability allowed an attacker to perform a remote code execution attack on affected servers.
- Affected Products: **Apache Tomcat 9.0.0.M1 to 9.0.17**
  Apache Tomcat 8.5.0 to 8.5.39
  Apache Tomcat 7.0.0 to 7.0.93
- Officially Acknowledged by the Vendor: **Yes**

VPN

- Multiple VPN applications from several vendors stores application and session cookies in an insecure manner in a machine' s memory and logs. An attacker, if able to steal the cookies could perform a session replay attack and bypass other authentication methods, allowing the attacker to access applications available to the victim user.
- Affected Products: **Palo Alto Networks GlobalProtect Agent 4.1.0 for Windows and GlobalProtect Agent 4.1.10 and earlier for macOS0**
  Pulse Secure Connect Secure prior to 8.1R14, 8.2, 8.3R6, and 9.0R2
  Cisco AnyConnect 4.7.x and prior
  F5 Networks multiple products and versions
- Officially Acknowledged by the Vendor: **Palo Alto – Yes, Pulse Secure – Yes, Cisco – No, F5 Networks - Yes**

Joomla

- Joomla has issues a security announcement and fix to resolve a directory traversal issue through their Media manager component. An attacker could use this flaw to operate outside the root directory of media manager.
- Affected Products: **Joomla CMS versions 1.5.0 through 3.9.4**
- Officially Acknowledged by the Vendor: **Yes**

WAP3

- Issues have been identified with the WAP3 protocol's design. The implementation of "hostapd" and "wpa_supplicant" allows a remote attacker to acquire weak passwords, conduct denial of service attacks or gain complete authorization.
- Affected Products: **N/A**
- Officially Acknowledged by the Vendor: **N/A**

Microsoft Support Agent Hacked

- Attackers have been able to successfully attack Microsoft Support Agent and gained access to the agent. Through this attack, the attackers are able to view some information from some email accounts. Attackers however were **not** able to see email content or attachments.
- Affected Products: **Outlook.com**
- Officially Acknowledged by the Vendor: **Yes**

Additional Information

Visit the links below and follow the instructions given by respective vendors.

Apache Tomcat

- http://mail-archives.us.apache.org/mod_mbox/www-announce/201904.mbox/%3C13d878ec-5d49-c348-48d4-25a6c81b9605%40apache.org%3E

VPN

- https://securityadvisories.paloaltonetworks.com/Home/Detail/146?AspxAutoDetectCookieSupport=1
- https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44114/
- https://support.f5.com/csp/article/K45432295

Joomla

- https://developer.joomla.org/security-centre/777-20190401-core-directory-traversal-in-com-media

WAP3

- https://thehackernews.com/2019/04/wpa3-hack-wifi-password.html

Microsoft Support Agent Hacked

- https://thehackernews.com/2019/04/microsoft-outlook-email-hack.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.