AESDDoS bot exploits CVE-2019-3396 flaw to hit Atlassian Confluence Server

April 28, 2019 By Pierluigi Paganini

https://securityaffairs.co/wordpress/84591/malware/aesddos-bot-atlassian-confluence.html

A new variant of the AESDDoS bot is exploiting a recent vulnerability in the Atlassian collaborative software Confluence.

Security experts at Trend Micro have spotted a new variant of AESDDoS botnet that is exploiting a recently discovered vulnerability in the Atlassian collaborative software Confluence.

The flaw exploited in the attacks, tracked as CVE-2019-3396, is a server-side template injection vulnerability that resides in the Widget Connector macro in Confluence Server.

Threat actors leverage the vulnerability to install denial of service (DDoS) malware and crypto-currency miners, and to remotely execute code.

"In our analysis, we saw that an attacker was able to exploit CVE-2019-3396 to infect machines with the AESDDoS botnet malware." reads the analysis published by Trend Micro. "A shell command was remotely executed to download and execute a malicious shell script (Trojan.SH.LODEX.J), which in turn downloaded another shell script (Trojan.SH.DOGOLOAD.J) that finally installed the AESDDoS botnet malware on the affected system."

The AESDDoS bot involved in the recent attacks has the ability to launch several types of DDoS attacks, including SYN, LSYN, UDP, UDPS, and TCP flood.

The malware also connects to 23.224.59.34:48080 to send and receive remote shell commands from the attacker.

Once the malware has infected a system, it can gather system information, including model ID and CPU description, speed, family, model, and type.

The AESDDoS bot uses the AES algorithm to encrypt gathered data and data received from the C2 server.

Trend Micro researchers also discovered that the latest variant of the AESDDoS bot can modify files i.e., /etc/rc.local and /etc/rc.d/rc.local, as an autostart technique by appending the {malware path}/{malware file name} reboot command.

Atlassian has already addressed the vulnerability in the Confluence software with the release of the version 6.15.1.

"Since the successful exploitation of CVE-2019-3396 in Atlassian Confluence Server can put resources at risk, enterprises should be able to identify vulnerabilities, make use of the latest threat intelligence against malware or exploits, and detect modifications to the application's design and the underlying infrastructure that hosts it," Trend Micro concludes.

Pierluigi Paganini

SecurityAffairs – AESDDoS bot, DDoS