Security Advisory Report - OBSO-1708-01

Linux Kernel Stack Guard Page Security Feature Bypass Weakness (CVE-2017-1000364)

Creation Date: 2017-07-21 16:42:43
Last Update: 2018-08-22 12:01:15

Summary

Update: most products have a fix now, see below

A new Linux Kernel vulnerability was discovered by Qualys:

The stack guard page security mechanism was found to be insufficient.
The size of the stack guard gap was increased from a single page to 256 pages

A flaw was found in the way memory was being allocated on the stack for user space binaries. If heap (or different memory region) and stack memory regions were adjacent to each other, an attacker could use this flaw to jump over the stack guard gap, cause controlled memory corruption on process stack or the adjacent memory region, and thus increase their privileges on the system. This is a kernel-side mitigation which increases the stack guard gap size from one page to 256 pages to make successful exploitation of this issue more difficult.

This vulnerability requires a local access to be exploited.

Exploits and PoCs are available.

CVSS v2 base score 6.2 Medium

https://nvd.nist.gov/vuln/detail/CVE-2017-1000364

Details

Linux Kernel contains a limitation in the stack guard page security mechanism, which creates a 4KB stack guard page at the start of the stack to protect against stack clash type vulnerabilities relying on sequential overwrites.

An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).

The issue is triggered as certain types of vulnerabilities in other software that grant a large amount of control over stack memory allocations may bypass the protection by jumping the stack guard page gap.

The concept of stack clash type vulnerabilities was first described by Gael Delalleau in his 2005 presentation at CanSecWest. The problem was revisited by Rafal Wojtczuk in 2010. In response to this, the Linux kernel developers introduced the stack guard page security feature (a 4K non-writable page below the start of the stack) in 2010 to reduce the risk of attacks via sequential overwrites.

The stack guard page security feature should be considered a "best effort" security feature similar to most other security features introduced in modern OS to reduce the risk of successful memory corruption attacks. These are in no way a panacea. The latest fix also just increases the size of the stack guard gap from a single page to 256 pages i.e. a 1MiB (mebyte = 1 048 576 bytes) gap. This makes exploitation of non-sequential stack clash attacks harder, but still only mitigates the risk and does not remove it completely, depending on the vulnerabilities that exist in other programs. The best approach to prevent stack clash type vulnerabilities is to compile all code using the -fstack-check GCC compiler option.

While this does not constitute a vulnerability in the Linux kernel, RBS still recommends to apply fixes in a timely manner. These reduce the risk of stack clash type vulnerabilities that may affect a large number of setuid programs.

The attack vector has been classified as Location Unknown. The most plausible vector is local, but there may be some software providing remote vectors by allowing a great amount of control over stack memory allocations. It should be noted that this would be considered a vulnerability in these programs and not the Linux kernel.

Normally, issues that are not considered legitimate vulnerabilities receive a CVSS score of 0.0. However, to ensure this entry receives proper attention, an exception was made. It has been assigned a CVSSv2 score based on the most plausible impact of stack clash type vulnerabilities in general. In some cases of stack clash type vulnerabilities, it should also be noted that a combination of multiple non-issues could combined result in a valid security impact. In such cases, the best mitigation would be to apply the stack guard fix to the underlying OS, which the assigned CVSSv2 score captures.

Affected Products

Affected products, fix available
OpenScape Voice V8 R1 fixed in V9 R2.24.6: Single Load Line
OpenScape Voice V9 fixed in V9 R2.24.6

Circuit Server fixed in Sprint 78

OpenScape 4000 V7 fixed in V7 R2.24
OpenScape 4000 V8 fixed in V8 R1.19

OpenScape Desk Phone CP SIP fixed in V1 R3.6.0
OpenScape Desk Phone CP HFA fixed in V1 R1.12.0
OpenScape Desk Phone IP 35G Eco SIP fixed in V3 R5.7.0

OpenScape Desk Phone IP 35G Eco HFA fixed in V3 R0.39.4

OpenStage Xpert 6010p turret (Linux) V6 R1.1.0
OpenStage Xpert 6010p turret (Linux) V5 R1.6.6

Circuit Meeting Room fixed in V1 R3.4.0

Affected products, fix in work:

OpenScape Branch/SBC V8 R1 fix in work, planned for V9 R4
OpenScape Branch/SBC V9 fix in work, planned for V9 R4

OpenStage 15/20E/20/40 and OpenScape Desk Phone IP 35G SIP
OpenStage 15/20E/20/40 and OpenScape Desk Phone IP 35G HFA
OpenStage 60 and OpenScape Desk Phone IP 35G SIP
OpenStage 60 and OpenScape Desk Phone IP 35G HFA

Not affected products
OpenScape Business S V2: with applications customer performs patching.

Recommended Actions

Patches for Linux should be applied where available.

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-1000364

https://nvd.nist.gov/vuln/detail/CVE-2017-1000364

http://thehackernews.com/2017/06/linux-root-privilege-escalation.html

https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt?_ga=2.21132280.2111220318.1497939003-1499227004.1497422555

https://blog.qualys.com/securitylabs/2017/06/19/the-stack-clash

http://seclists.org/bugtraq/2017/Jun/37

http://lists.opensuse.org/opensuse-security-announce/2017-06/msg00012.html

https://www.suse.com/support/update/announcement/2017/suse-su-20171613-1/

http://rhn.redhat.com/errata/RHSA-2017-1482.html

https://www.redhat.com/archives/rhsa-announce/2017-June/msg00052.html

https://threatpost.com/stack-clash-vulnerability-in-linux-bsd-systems-enables-root-access/126355/

http://www.securityfocus.com/bid/99130

Advisory: OBSO-1708-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com