CRITICAL VULNERABILITY
OPENSSL 3.0.X

WHAT IS OPENSSL AND WHERE IS IT USED?

OpenSSL is an open-source library used to encrypt communications between servers and clients. It is used in nearly all operating systems but is especially present in Linux distributions.

IN SHORT

CHECK — Find out if and where you use OpenSSL 3.0.x.

PLAN — Make a plan to update quickly as OpenSSL 3.0.7 becomes available.

ACT — Know what you need to do if an exploit becomes available before your systems are updated.

WHAT ARE THE CONSEQUENCES OF THIS VULNERABILITY?

There aren't many details available yet. All we know is that OpenSSL has branded the update as Critical (the highest rating OpenSSL uses). This means that OpenSSL thinks the vulnerability can be easily exploited in common situations, leading to compromise of private keys or remote code execution. There is no CVE available yet, but we expect the CVE score to be somewhere between 9 and 10.

WHAT CAN I DO TO PREVENT SOMEONE FROM ABUSING THIS VULNERABILITY?

Since information is scarce, we don't think the vulnerability is being exploited, yet. OpenSSL will release version 3.0.7 on Tuesday 1st November 2022 between 1500-1900 Amsterdam Time. Make sure you have a plan to quickly update after the update becomes available, since exploits are to be expected shortly after release. It is wise to have a plan ready, should an exploit become available before 1st November.

HOW DO I KNOW IF MY SYSTEMS ARE VULNERABLE?

Currently, it seems that only OpenSSL versions 3.0 and higher are vulnerable. On most operating systems you can use the command `"openssl version"` to check your version. Software packages usually use their own crypto-graphical implementations. However, there may be cases where OpenSSL is used through third party packages or in containers.

CAN I GET INFORMATION DIRECTLY FROM OPENSSL?

OpenSSL has only made a single announcement on their mailing list. You can check the OpenSSL.org vulnerabilities page for updates.

OUR TECHBURST BLOG: WWW.TEAMROCKSTARS.NL/DEVELOPERS/TECH-BURST/

OPENSSL VULNERABILITIES PAGE: WWW.OPENSSL.ORG/NEWS/VULNERABILITIES.HTML