Advisory Alert

Alert Number: AAA20201104 **Date:** November 4, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	CVE-2020-14871 :Zero-day vulnerability (AAA20201021)

Description

Affected Product	**Oracle**
Severity	**Critical -** Initial release date is 21st Oct 2020. This patch is again sent as a reminder to update since there are recent exploitation attempts of this vulnerability throughout the world.
Affected Vulnerability	Multiple vulnerabilities
Description	A new threat actor called UNC1945, is actively exploits a vulnerability in the Solaris Pluggable Authentication Module (PAM) that allowed UNC1945 to bypass authentication procedures and install a backdoor named SLAPSTICK on internet-exposed Solaris servers using EVILSUN - a remote exploitation tool that gains access to Solaris 10 and 11 systems of SPARC or i386 architecture using a vulnerability (CVE-2020-14871) exposed by SSH keyboard-interactive authentication. Oracle has released its October 2020 Critical patch update containing a collection of patches to address several security vulnerabilities affected by multiple products which include the CVE-2020-14871 which is the vulnerability UNC1945 is using to exploit.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuoct2020.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.