ALE Security Advisory	No. SA-A0010	Ed. 02

CVE-2024-6387 related to OpenSSH

Summary

Several vulnerabilities have been discovered in OpenSSH. They allow an unauthenticated remote attacker to take the full control of a vulnerable system.

References

Reference	CVE-2024-6397
Date	11/07/2024
Risk	Very High
Impact	take control, execute_arbitrary_code, confidentiality
Attack expertise	skilled, remote_no_account_no_user_interaction
Attack requirements	
CVSS score	8.1
Affected versions	OpenSSH versions 8.5 and later, and prior to 9.8
Fixed version	9.8

Description of the vulnerability

Several vulnerabilities have been discovered in OpenSSH. They allow an unauthenticated remote attacker to take the full control of a vulnerable system to execute arbitrary code to illegally take knowledge of potentially sensitive data.
Note: An exploit has been published on the Internet for the CVE-2024-6387 vulnerability. Qualys (discoverer of the vulnerability) reports that the CVE-2024-6387 vulnerability is a regression of the CVE-2006-5051 vulnerability (which was patched in 2006) and has named this vulnerability regreSSHion

Impacts

Take control, change scope, corrupt system, access to sensitive data

Status on Alcatel-Lucent Enterprise Communication products

List of products and releases

Products	Versions	Affected	Impact	Remediation
Cloud Connect		0		
FlexLM	3.0.000.001-3.0.000.007	**Yes**	N/A	dnf update
OmniPCX Enterprise CS	R101	**Yes**		
OmniPCX Enterprise OMS	All	No	N/A	N/A
OmniPCX Enterprise GD3	All	NO	N/A	N/A
OmniPCX Enterprise GD4	All	**Yes**		
OmniPCX Enterprise OST-EEGW	All	No	N/A	N/A
OmniVista 8770	All	No	N/A	N/A
BootDVD	All	No	N/A	N/A
OpenTouch	All	No	N/A	N/A
GAS Server OS		Under Evaluation		
VAA	All	No	N/A	N/A
VNA		0		
O2G	All	No	N/A	N/A
4059EE	All	No	N/A	N/A
4059IP		0		
IPDongle (RPi)		0		
ALE Softphone PC	All	No	N/A	N/A
ALE Softphone mobile	All	No	N/A	N/A
OTC Client PC	All	No	N/A	N/A
OTC Client mobile	All	No	N/A	N/A
OTSBC	All	No	N/A	N/A
ALE Connect	All	No	N/A	N/A
CCIVR / CCS / CCA	All	No	N/A	N/A
ASM (Agent Selection Module)	All	No	N/A	N/A
OmniPCX Record	All	No	N/A	N/A
IP Desktop SoftPhone	All	No	N/A	N/A
ManageMyPhone	All	No	N/A	N/A
SelfCare	All	No	N/A	N/A
AVBS	All	No	N/A	N/A
Dispatch Console	All	No	N/A	N/A
OmniPCX Office	All	No	N/A	N/A
OXO Connect	All	No	N/A	N/A
OXO Connect Evolution	All	No	N/A	N/A
OCE Front-End	All	No	N/A	N/A
OMC / OHL / OLD / PIMPhony / AST / LabelSet	All	No	N/A	N/A
8088	All	No	N/A	N/A
8008 / 8008G / 8018 / 80x8s	All	No	N/A	N/A
ALE Enterprise DeskPhones (ALE-500 / 400 / 300) - NOE	All	**Yes**	N/A	R310
ALE Enterprise DeskPhones (ALE-500 / 400 / 300) - SIP	All	**Yes**	N/A	R400
ALE Essential DeskPhones (ALE-30H / 20H / 20) - NOE	All	**Yes**	N/A	R310

ALE-2 / ALE-3	All	**Yes**	N/A	R400
EDS / EPS / EDM	All	No	N/A	N/A
8008-CE / 8008G-CE / 8018 CE / 80x8s CE	All	No	N/A	N/A
M3 / M5 / M7	All	No	N/A	N/A
H2	All	No	N/A	N/A
H3 / H6 / M8	All	**Yes**	High	R400
EM20 / EM200	All	No	N/A	N/A

3rd Party

3rd Party Products	*Versions*	*Affected*	*Impact*	*Remediation*
FlexLM	3.0.000.001-3.0.000.006	**Yes**	N/A	dnf update

Status on Alcatel-Lucent Enterprise Network products

Products	Versions	Affected	Impact	Remediation
Subscription Manager	All	No	N/A	N/A
Agnostic Data Lake	All	No	N/A	N/A
Asset Tracking	All	No	N/A	N/A
OV Cirrus (4.x)	All	No	N/A	N/A
OV Cirrus (1x.x)	All	No	N/A	N/A
OV 2500	All	No	N/A	N/A
RAP Appliance	All	No	N/A	N/A
OmniSwitch AOS 5 (2x60)	5.x	No	N/A	N/A
OmniSwitch AOS 6 (6250, 6350, 6450)	6.x	No	N/A	N/A
OmniSwitch AOS 8 (6360, 6465, 6560, 6570, 6860, 6865, 6900, 9900)	8.8.R01 thru 8.9.R04	**Yes**	High	See section OmniSwitch AOS 8
OmniAccess Stellar AP	All	No	N/A	N/A
OmniAccess WLAN APs & Controllers	All	No	N/A	N/A
OV 3600	8.3.0.2 and below	Yes	Medium	Under investigation
ClearPass Policy Manager	All	No	N/A	N/A
OmniVista Network Advisor	All	No	N/A	N/A

Status on Alcatel Lucent Enterprise Rainbow solutions

List of products and releases

Products	Versions	Affected	Impact	Remediation
Rainbow UCaaS/CPaaS/Edge/HDS/Hub		No		

OmniSwitch AOS 8

Affected Versions: The vulnerability impacts OmniSwitch products using AOS 8.8.R01 through AOS 8.9.R04. Earlier versions of AOS 8 are not impacted.

Best Practice: Management access to the OmniSwitch should be limited to a network segment that is protected by firewall policy rules and where access is restricted to authorized network administration personnel.

Workaround: The workaround is to Set "LoginGraceTime" to "0" in sshd_cfg.

- AOS 8.10.R1 expected in July 2024 enables the workaround by default. If the “ssh login-grace-time ” is already configured to a value other than 0, it is advisable to set to “0” using “ssh login-grace-time 0”.
- For earlier versions of AOS contact ALE Customer Support for assistance.

Remediation: Full remediation is in AOS 8.10.R02 expected December 2024

History

01	July 11th 2024	creation
02	July 15th 2024	Update