PSIRT Advisories

ID STW-IR-24-001

Published 11.07.2024 13:28 (CEST)

Last update none

Severity High

CVSSv3 Score 8.1

Product(s)

Article Number	Product Name	Affected Version(s)
any	TCG-4 TCG-4lite	<= DeploymentPackage_v3_08r1-Monkey
104581, 107333, 107336, 108049, 108053	ESX.4CL-p ESX.4CL-ag-p	<= DeploymentPackage_v3_08r1-Monkey

Summary

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

We upgraded the openssh version to 9.8p1 to get the latest security fixes.

CVE ID CVE-2024-16387

Impact An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

Affected Components

- sshd (OpenSSH's server)

Solution Please upgrade to
DeploymentPackage_v3_08r1-Monkey (TCG-4)
DeploymentPackage_v3_08r1-Monkey (TCG-4lite)
DeploymentPackage_v3_08r1-Monkey (ESX.4cl-p/ESX.4cl-ag-p)

If deployment package cannot be updated to Monkey (v3.08r1), security researchers recommend setting parameter '*LoginGraceTime*' to '*0*' in the config file of sshd. This exposes sshd to a denial of service by using up all '*MaxStartups*' connections, but it prevents the remote code execution risk.

Address
Am Bärenwald 6
87600 Kaufbeuren
Germany
Internet
www.stw-mm.com

Phone
+49 8341 9505-0
Fax
+49 8341 9505-55
E-Mail
info.stw@wiedemann-group.com

Registered office
Kaufbeuren
Register court
Kempten HRB 1863

Managing Directors
Sonja Wiedemann
Christophe de Bary
Michael Otto

VAT. Reg. No.
DE 811 355 522

Bank details
Baden-Württembergische Bank
IBAN DE11 6005 0101 0004 1026 67
BIC SOLADEST600

Bank details
Sparkasse Allgäu
IBAN DE29 7335 0000 0000 0219 72
BIC BYLADEM1ALG