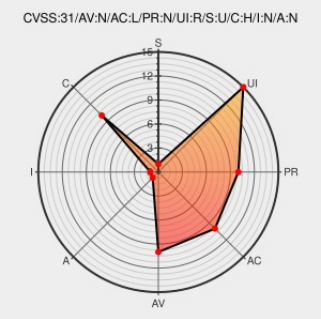
CVE-2022-29245

Published on: Not Yet Published

Last Modified on: 11/07/2023 03:45:00 AM UTC

CVE-2022-29245 - advisory for GHSA-72p8-v4hg-v45p

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ssh.net from Ssh.net Project contain the following vulnerability:

SSH.NET is a Secure Shell (SSH) library for .NET. In versions 2020.0.0 and 2020.0.1, during an `X25519` key exchange, the client's private key is generated with `System.Random`. `System.Random` is not a cryptographically secure random number generator, it must therefore not be used for cryptographic purposes. When establishing an SSH connection to a remote host, during the X25519 key exchange, the private key is generated with a weak random number generator whose seed can be brute forced. This allows an attacker who is able to eavesdrop on the communications to decrypt them. Version 2020.0.2 contains a patch for this issue. As a workaround, one may disable support for `curve25519-sha256` and `curve25519-sha256@libssh.org` key exchange algorithms.

CVE-2022-29245 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **sshnet** - **SSH.NET** version **>= 2020.0.0, < 2020.0.2**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Weak private key generation · Advisory · sshnet/SSH.NET · GitHub	github.com text/html	CONFIRM github.com/sshnet/SSH.NET/security/advisories/GHSA-72p8-v
Release 2020.0.2 · sshnet/SSH.NET · GitHub	github.com text/html	MISC github.com/sshnet/SSH.NET/releases/tag/2020.0.2
Use cryptographically secure random number generator. · sshnet/SSH.NET@03c6d60 · GitHub	github.com text/html	MISC github.com/sshnet/SSH.NET/commit/03c6d60736b8f7b42e44d6989
SSH.NET/KeyExchangeECCurve25519.cs at bc99ada7da3f05f50d9379f2644941d91d5bf05a · sshnet/SSH.NET · GitHub	github.com text/html	MISC github.com/sshnet/SSH.NET/blob/bc99ada7da3f05f50d9379f2644941d91d5b

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ssh.net Project	Ssh.net	2020.0.0	-	All	All
Application	Ssh.net Project	Ssh.net	2020.0.0	beta1	All	All
Application	Ssh.net Project	Ssh.net	2020.0.1	All	All	All

cpe:2.3:a:ssh.net_project:ssh.net:2020.0.0:-:*:*:*:.net:*:*:

cpe:2.3:a:ssh.net_project:ssh.net:2020.0.0:beta1:*:*:*:.net:*:*:

cpe:2.3:a:ssh.net_project:ssh.net:2020.0.1:*:*:*:*:.net:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29245 : SSH.NET is a Secure Shell SSH library for .NET. In versions 2020.0.0 and 2020.0.… twitter.com/i/web/status/1…	2022-05-31 16:40:27
@0_exploit	CVE-2022-29245 dlvr.it/SRNySS	2022-05-31 20:29:05
/r/netcve	CVE-2022-29245	2022-05-31 17:38:12

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report