



# CVE-2022-29245

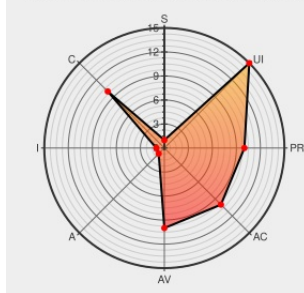
Published on: Not Yet Published

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](#)

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



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  $\geq 2020.0.0$ ,  $< 2020.0.2$

CVSS3 Score: **5.9 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
|                        |                   |                     |

PARTIAL

NONE

NONE

## CVE References

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type        | Vendor                          | Product                 | Version  | Update | Edition | Language |
|-------------|---------------------------------|-------------------------|----------|--------|---------|----------|
| Application | <a href="#">Ssh.net Project</a> | <a href="#">Ssh.net</a> | 2020.0.0 | -      | All     | All      |
| Application | <a href="#">Ssh.net Project</a> | <a href="#">Ssh.net</a> | 2020.0.0 | beta1  | All     | All      |
| Application | <a href="#">Ssh.net Project</a> | <a href="#">Ssh.net</a> | 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 : <a href="#">SSH.NET</a> is a Secure Shell SSH library for .NET. In versions 2020.0.0 and 2020.0.... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-05-31<br>16:40:27 |
|  @0_exploit | CVE-2022-29245 <a href="https://dlvr.it/SRNySS">dlvr.it/SRNySS</a>                                                                                                                                     | 2022-05-31<br>20:29:05 |
|  /r/netcve  | <a href="#">CVE-2022-29245</a>                                                                                                                                                                         | 2022-05-31<br>17:38:12 |

© CVE.report 2024   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)