# Отчет по безопасности сети 127.0.0.1/24

## Служебная информация:

Дата сканирования: 2024-01-12 20:45:25

Версия сканера: 1.0

Режим сканирования: TCP

Режим CVE: True

Режим сканирования всех портов: False

## Общая информация о сетевых узлах:

|  |  |  |  |
| --- | --- | --- | --- |
| Ip Адрес узла | Состояние хоста | Количество открытых портов | Общее количество CVE |
| 127.0.0.32 | up | 1 | 12 |
| 127.0.0.0 | up | 1 | 12 |
| 127.0.0.64 | up | 1 | 12 |
| 127.0.0.33 | up | 1 | 12 |
| 127.0.0.65 | up | 1 | 12 |
| 127.0.0.34 | up | 1 | 12 |
| 127.0.0.66 | up | 1 | 12 |
| 127.0.0.35 | up | 1 | 12 |
| 127.0.0.67 | up | 1 | 12 |
| 127.0.0.36 | up | 1 | 12 |
| 127.0.0.68 | up | 1 | 12 |
| 127.0.0.1 | up | 4 | 69 |
| 127.0.0.37 | up | 1 | 12 |
| 127.0.0.69 | up | 1 | 12 |
| 127.0.0.2 | up | 1 | 12 |
| 127.0.0.38 | up | 1 | 12 |
| 127.0.0.70 | up | 1 | 12 |
| 127.0.0.3 | up | 1 | 12 |
| 127.0.0.39 | up | 1 | 12 |
| 127.0.0.71 | up | 1 | 12 |
| 127.0.0.4 | up | 1 | 12 |
| 127.0.0.40 | up | 1 | 12 |
| 127.0.0.72 | up | 1 | 12 |
| 127.0.0.5 | up | 1 | 12 |
| 127.0.0.41 | up | 1 | 12 |
| 127.0.0.73 | up | 1 | 12 |
| 127.0.0.6 | up | 1 | 12 |
| 127.0.0.42 | up | 1 | 12 |
| 127.0.0.74 | up | 1 | 12 |
| 127.0.0.43 | up | 1 | 12 |
| 127.0.0.7 | up | 1 | 12 |
| 127.0.0.75 | up | 1 | 12 |
| 127.0.0.44 | up | 1 | 12 |
| 127.0.0.8 | up | 1 | 12 |
| 127.0.0.76 | up | 1 | 12 |
| 127.0.0.45 | up | 1 | 12 |
| 127.0.0.9 | up | 1 | 12 |
| 127.0.0.77 | up | 1 | 12 |
| 127.0.0.46 | up | 1 | 12 |
| 127.0.0.10 | up | 1 | 12 |
| 127.0.0.78 | up | 1 | 12 |
| 127.0.0.47 | up | 1 | 12 |
| 127.0.0.11 | up | 1 | 12 |
| 127.0.0.79 | up | 1 | 12 |
| 127.0.0.12 | up | 1 | 12 |
| 127.0.0.48 | up | 1 | 12 |
| 127.0.0.80 | up | 1 | 12 |
| 127.0.0.13 | up | 1 | 12 |
| 127.0.0.49 | up | 1 | 12 |
| 127.0.0.81 | up | 1 | 12 |
| 127.0.0.14 | up | 1 | 12 |
| 127.0.0.50 | up | 1 | 12 |
| 127.0.0.82 | up | 1 | 12 |
| 127.0.0.15 | up | 1 | 12 |
| 127.0.0.51 | up | 1 | 12 |
| 127.0.0.83 | up | 1 | 12 |
| 127.0.0.16 | up | 1 | 12 |
| 127.0.0.52 | up | 1 | 12 |
| 127.0.0.84 | up | 1 | 12 |
| 127.0.0.53 | up | 2 | 12 |
| 127.0.0.17 | up | 1 | 12 |
| 127.0.0.85 | up | 1 | 12 |
| 127.0.0.54 | up | 1 | 12 |
| 127.0.0.18 | up | 1 | 12 |
| 127.0.0.86 | up | 1 | 12 |
| 127.0.0.55 | up | 1 | 12 |
| 127.0.0.19 | up | 1 | 12 |
| 127.0.0.87 | up | 1 | 12 |
| 127.0.0.56 | up | 1 | 12 |
| 127.0.0.20 | up | 1 | 12 |
| 127.0.0.88 | up | 1 | 12 |
| 127.0.0.57 | up | 1 | 12 |
| 127.0.0.21 | up | 1 | 12 |
| 127.0.0.89 | up | 1 | 12 |
| 127.0.0.58 | up | 1 | 12 |
| 127.0.0.22 | up | 1 | 12 |
| 127.0.0.90 | up | 1 | 12 |
| 127.0.0.23 | up | 1 | 12 |
| 127.0.0.59 | up | 1 | 12 |
| 127.0.0.91 | up | 1 | 12 |
| 127.0.0.24 | up | 1 | 12 |
| 127.0.0.60 | up | 1 | 12 |
| 127.0.0.92 | up | 1 | 12 |
| 127.0.0.25 | up | 1 | 12 |
| 127.0.0.61 | up | 1 | 12 |
| 127.0.0.93 | up | 1 | 12 |
| 127.0.0.26 | up | 1 | 12 |
| 127.0.0.62 | up | 1 | 12 |
| 127.0.0.94 | up | 1 | 12 |
| 127.0.0.27 | up | 1 | 12 |
| 127.0.0.63 | up | 1 | 12 |
| 127.0.0.95 | up | 1 | 12 |
| 127.0.0.28 | up | 1 | 12 |
| 127.0.0.29 | up | 1 | 12 |
| 127.0.0.30 | up | 1 | 12 |
| 127.0.0.96 | up | 1 | 12 |
| 127.0.0.128 | up | 1 | 12 |
| 127.0.0.97 | up | 1 | 12 |
| 127.0.0.31 | up | 1 | 12 |
| 127.0.0.129 | up | 1 | 12 |
| 127.0.0.98 | up | 1 | 12 |
| 127.0.0.99 | up | 1 | 12 |
| 127.0.0.130 | up | 1 | 12 |
| 127.0.0.131 | up | 1 | 12 |
| 127.0.0.160 | up | 1 | 12 |
| 127.0.0.161 | up | 1 | 12 |
| 127.0.0.132 | up | 1 | 12 |
| 127.0.0.162 | up | 1 | 12 |
| 127.0.0.133 | up | 1 | 12 |
| 127.0.0.134 | up | 1 | 12 |
| 127.0.0.163 | up | 1 | 12 |
| 127.0.0.135 | up | 1 | 12 |
| 127.0.0.164 | up | 1 | 12 |
| 127.0.0.100 | up | 1 | 12 |
| 127.0.0.101 | up | 1 | 12 |
| 127.0.0.102 | up | 1 | 12 |
| 127.0.0.103 | up | 1 | 12 |
| 127.0.0.104 | up | 1 | 12 |
| 127.0.0.136 | up | 1 | 12 |
| 127.0.0.165 | up | 1 | 12 |
| 127.0.0.105 | up | 1 | 12 |
| 127.0.0.137 | up | 1 | 12 |
| 127.0.0.166 | up | 1 | 12 |
| 127.0.0.106 | up | 1 | 12 |
| 127.0.0.167 | up | 1 | 12 |
| 127.0.0.138 | up | 1 | 12 |
| 127.0.0.107 | up | 1 | 12 |
| 127.0.0.168 | up | 1 | 12 |
| 127.0.0.139 | up | 1 | 12 |
| 127.0.0.108 | up | 1 | 12 |
| 127.0.0.169 | up | 1 | 12 |
| 127.0.0.140 | up | 1 | 12 |
| 127.0.0.109 | up | 1 | 12 |
| 127.0.0.170 | up | 1 | 12 |
| 127.0.0.141 | up | 1 | 12 |
| 127.0.0.110 | up | 1 | 12 |
| 127.0.0.171 | up | 1 | 12 |
| 127.0.0.142 | up | 1 | 12 |
| 127.0.0.111 | up | 1 | 12 |
| 127.0.0.172 | up | 1 | 12 |
| 127.0.0.173 | up | 1 | 12 |
| 127.0.0.143 | up | 1 | 12 |
| 127.0.0.144 | up | 0 | 10 |
| 127.0.0.112 | up | 1 | 12 |
| 127.0.0.113 | up | 0 | 6 |

## Подробная информация о сетевых узлах:

### Узел 127.0.0.32/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.0/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.64/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.33/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.65/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.34/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.66/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.35/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.67/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.36/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.68/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.1/24

Состояние: up

Количество открытых портов: 4

Общее количество CVE: 69

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |
| 631 | open | syn-ack | ipp | [CVE-2019-12584] - Средняя [CVE-2019-12585] - Критичная [CVE-2023-32324] - Средняя [CVE-2023-34241] - Высокая [CVE-2023-4504] - Высокая [CVE-2002-1384] - Высокая [CVE-2004-0888] - Критичная [CVE-2004-1270] - Низкая [CVE-2007-3387] - Средняя [CVE-2007-4045] - Средняя [CVE-2009-0032] - Средняя [CVE-2009-0791] - Средняя [CVE-2011-2896] - Средняя [CVE-2014-5030] - Низкая [CVE-2014-5031] - Средняя [CVE-2014-9679] - Средняя [CVE-2015-1158] - Критичная [CVE-2015-1159] - Средняя [CVE-2017-18190] - Высокая [CVE-2017-18248] - Средняя [CVE-2018-6553] - Высокая [CVE-2020-4060] - Средняя |
| 5432 | open | syn-ack | postgresql | [CVE-2009-0696] - Средняя [CVE-2014-125105] - Средняя [CVE-2017-10086] - Критичная [CVE-2017-10089] - Критичная [CVE-2017-10110] - Критичная [CVE-2017-12172] - Средняя [CVE-2017-15098] - Высокая [CVE-2017-15099] - Средняя [CVE-2017-7484] - Высокая [CVE-2017-7485] - Средняя [CVE-2017-7486] - Высокая [CVE-2017-7546] - Критичная [CVE-2017-7547] - Высокая [CVE-2017-7548] - Высокая [CVE-2018-1053] - Высокая [CVE-2018-10915] - Высокая [CVE-2018-10925] - Высокая [CVE-2018-1115] - Критичная [CVE-2018-7210] - Высокая [CVE-2019-10130] - Средняя [CVE-2019-10208] - Высокая [CVE-2019-10210] - Высокая [CVE-2019-10211] - Критичная [CVE-2019-25094] - Средняя [CVE-2020-14350] - Высокая [CVE-2020-1720] - Средняя [CVE-2020-25694] - Высокая [CVE-2020-25695] - Высокая [CVE-2020-25696] - Высокая [CVE-2021-32027] - Высокая [CVE-2021-37665] - Высокая [CVE-2022-3952] - Высокая [CVE-2012-1618] - Высокая [CVE-2014-0067] - Средняя [CVE-2016-5424] - Высокая |
| 8000 | open | syn-ack | http-alt |  |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.  
  
  
  
update\_cve.csv:  
[CVE-2019-12584] Apcupsd 0.3.91\_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an XSS issue in apcupsd\_status.php.  
  
[CVE-2019-12585] Apcupsd 0.3.91\_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an Arbitrary Command Execution issue in apcupsd\_status.php.  
  
[CVE-2023-32324] OpenPrinting CUPS is an open source printing system. In versions 2.4.2 and prior, a heap buffer overflow vulnerability would allow a remote attacker to launch a denial of service (DoS) attack. A buffer overflow vulnerability in the function `format\_log\_line` could allow remote attackers to cause a DoS on the affected system. Exploitation of the vulnerability can be triggered when the configuration file `cupsd.conf` sets the value of `loglevel `to `DEBUG`. No known patches or workarounds exist at time of publication.  
  
[CVE-2023-34241] OpenPrinting CUPS is a standards-based, open source printing system for Linux and other Unix-like operating systems. Starting in version 2.0.0 and prior to version 2.4.6, CUPS logs data of free memory to the logging service AFTER the connection has been closed, when it should have logged the data right before. This is a use-after-free bug that impacts the entire cupsd process. The exact cause of this issue is the function `httpClose(con->http)` being called in `scheduler/client.c`. The problem is that httpClose always, provided its argument is not null, frees the pointer at the end of the call, only for cupsdLogClient to pass the pointer to httpGetHostname. This issue happens in function `cupsdAcceptClient` if LogLevel is warn or higher and in two scenarios: there is a double-lookup for the IP Address (HostNameLookups Double is set in `cupsd.conf`) which fails to resolve, or if CUPS is compiled with TCP wrappers and the connection is refused by rules from `/etc/hosts.allow` and `/etc/hosts.deny`. Version 2.4.6 has a patch for this issue.  
  
[CVE-2023-4504] Due to failure in validating the length provided by an attacker-crafted PPD PostScript document, CUPS and libppd are susceptible to a heap-based buffer overflow and possibly code execution. This issue has been fixed in CUPS version 2.4.7, released in September of 2023.  
  
[CVE-2002-1384] Integer overflow in pdftops, as used in Xpdf 2.01 and earlier, xpdf-i, and CUPS before 1.1.18, allows local users to execute arbitrary code via a ColorSpace entry with a large number of elements, as demonstrated by cups-pdf.  
  
[CVE-2004-0888] Multiple integer overflows in xpdf 2.0 and 3.0, and other packages that use xpdf code such as CUPS, gpdf, and kdegraphics, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code, a different set of vulnerabilities than those identified by CVE-2004-0889.  
  
[CVE-2004-1270] lppasswd in CUPS 1.1.22, when run in environments that do not ensure that file descriptors 0, 1, and 2 are open when lppasswd is called, does not verify that the passwd.new file is different from STDERR, which allows local users to control output to passwd.new via certain user input that triggers an error message.  
  
[CVE-2007-3387] Integer overflow in the StreamPredictor::StreamPredictor function in xpdf 3.02, as used in (1) poppler before 0.5.91, (2) gpdf before 2.8.2, (3) kpdf, (4) kdegraphics, (5) CUPS, (6) PDFedit, and other products, might allow remote attackers to execute arbitrary code via a crafted PDF file that triggers a stack-based buffer overflow in the StreamPredictor::getNextLine function.  
  
[CVE-2007-4045] The CUPS service, as used in SUSE Linux before 20070720 and other Linux distributions, allows remote attackers to cause a denial of service via unspecified vectors related to an incomplete fix for CVE-2007-0720 that introduced a different denial of service problem in SSL negotiation.  
  
[CVE-2009-0032] CUPS on Mandriva Linux 2008.0, 2008.1, 2009.0, Corporate Server (CS) 3.0 and 4.0, and Multi Network Firewall (MNF) 2.0 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/pdf.log temporary file.  
  
[CVE-2009-0791] Multiple integer overflows in Xpdf 2.x and 3.x and Poppler 0.x, as used in the pdftops filter in CUPS 1.1.17, 1.1.22, and 1.3.7, GPdf, and kdegraphics KPDF, allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PDF file that triggers a heap-based buffer overflow, possibly related to (1) Decrypt.cxx, (2) FoFiTrueType.cxx, (3) gmem.c, (4) JBIG2Stream.cxx, and (5) PSOutputDev.cxx in pdftops/. NOTE: the JBIG2Stream.cxx vector may overlap CVE-2009-1179.  
  
[CVE-2011-2896] The LZW decompressor in the LWZReadByte function in giftoppm.c in the David Koblas GIF decoder in PBMPLUS, as used in the gif\_read\_lzw function in filter/image-gif.c in CUPS before 1.4.7, the LZWReadByte function in plug-ins/common/file-gif-load.c in GIMP 2.6.11 and earlier, the LZWReadByte function in img/gifread.c in XPCE in SWI-Prolog 5.10.4 and earlier, and other products, does not properly handle code words that are absent from the decompression table when encountered, which allows remote attackers to trigger an infinite loop or a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted compressed stream, a related issue to CVE-2006-1168 and CVE-2011-2895.  
  
[CVE-2014-5030] CUPS before 2.0 allows local users to read arbitrary files via a symlink attack on (1) index.html, (2) index.class, (3) index.pl, (4) index.php, (5) index.pyc, or (6) index.py.  
  
[CVE-2014-5031] The web interface in CUPS before 2.0 does not check that files have world-readable permissions, which allows remote attackers to obtains sensitive information via unspecified vectors.  
  
[CVE-2014-9679] Integer underflow in the cupsRasterReadPixels function in filter/raster.c in CUPS before 2.0.2 allows remote attackers to have unspecified impact via a malformed compressed raster file, which triggers a buffer overflow.  
  
[CVE-2015-1158] The add\_job function in scheduler/ipp.c in cupsd in CUPS before 2.0.3 performs incorrect free operations for multiple-value job-originating-host-name attributes, which allows remote attackers to trigger data corruption for reference-counted strings via a crafted (1) IPP\_CREATE\_JOB or (2) IPP\_PRINT\_JOB request, as demonstrated by replacing the configuration file and consequently executing arbitrary code.  
  
[CVE-2015-1159] Cross-site scripting (XSS) vulnerability in the cgi\_puts function in cgi-bin/template.c in the template engine in CUPS before 2.0.3 allows remote attackers to inject arbitrary web script or HTML via the QUERY parameter to help/.  
  
[CVE-2017-18190] A localhost.localdomain whitelist entry in valid\_host() in scheduler/client.c in CUPS before 2.2.2 allows remote attackers to execute arbitrary IPP commands by sending POST requests to the CUPS daemon in conjunction with DNS rebinding. The localhost.localdomain name is often resolved via a DNS server (neither the OS nor the web browser is responsible for ensuring that localhost.localdomain is 127.0.0.1).  
  
[CVE-2017-18248] The add\_job function in scheduler/ipp.c in CUPS before 2.2.6, when D-Bus support is enabled, can be crashed by remote attackers by sending print jobs with an invalid username, related to a D-Bus notification.  
  
[CVE-2018-6553] The CUPS AppArmor profile incorrectly confined the dnssd backend due to use of hard links. A local attacker could possibly use this issue to escape confinement. This flaw affects versions prior to 2.2.7-1ubuntu2.1 in Ubuntu 18.04 LTS, prior to 2.2.4-7ubuntu3.1 in Ubuntu 17.10, prior to 2.1.3-4ubuntu0.5 in Ubuntu 16.04 LTS, and prior to 1.7.2-0ubuntu1.10 in Ubuntu 14.04 LTS.  
  
[CVE-2020-4060] In LoRa Basics Station before 2.0.4, there is a Use After Free vulnerability that leads to memory corruption. This bug is triggered on 32-bit machines when the CUPS server responds with a message (https://doc.sm.tc/station/cupsproto.html#http-post-response) where the signature length is larger than 2 GByte (never happens in practice), or the response is crafted specifically to trigger this issue (i.e. the length signature field indicates a value larger than (2\*\*31)-1 although the signature actually does not contain that much data). In such a scenario, on 32 bit machines, Basic Station would execute a code path, where a piece of memory is accessed after it has been freed, causing the process to crash and restarted again. The CUPS transaction is typically mutually authenticated over TLS. Therefore, in order to trigger this vulnerability, the attacker would have to gain access to the CUPS server first. If the user chose to operate without authentication over TLS but yet is concerned about this vulnerability, one possible workaround is to enable TLS authentication. This has been fixed in 2.0.4.  
  
  
  
update\_cve.csv:  
[CVE-2009-0696] The dns\_db\_findrdataset function in db.c in named in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.  
  
[CVE-2014-125105] A vulnerability was found in Broken Link Checker Plugin up to 1.10.1 on WordPress. It has been declared as problematic. Affected by this vulnerability is the function options\_page of the file core/core.php of the component Settings Page. The manipulation of the argument exclusion\_list/blc\_custom\_fields leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.10.2 is able to address this issue. The patch is named 90615fe9b0b6f9e6fb254d503c302e53a202e561. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-230659.  
  
[CVE-2017-10086] Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).  
  
[CVE-2017-10089] Vulnerability in the Java SE component of Oracle Java SE (subcomponent: ImageIO). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).  
  
[CVE-2017-10110] Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).  
  
[CVE-2017-12172] PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, 9.5.x before 9.5.10, 9.4.x before 9.4.15, 9.3.x before 9.3.20, and 9.2.x before 9.2.24 runs under a non-root operating system account, and database superusers have effective ability to run arbitrary code under that system account. PostgreSQL provides a script for starting the database server during system boot. Packages of PostgreSQL for many operating systems provide their own, packager-authored startup implementations. Several implementations use a log file name that the database superuser can replace with a symbolic link. As root, they open(), chmod() and/or chown() this log file name. This often suffices for the database superuser to escalate to root privileges when root starts the server.  
  
[CVE-2017-15098] Invalid json\_populate\_recordset or jsonb\_populate\_recordset function calls in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, 9.5.x before 9.5.10, 9.4.x before 9.4.15, and 9.3.x before 9.3.20 can crash the server or disclose a few bytes of server memory.  
  
[CVE-2017-15099] INSERT ... ON CONFLICT DO UPDATE commands in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, and 9.5.x before 9.5.10 disclose table contents that the invoker lacks privilege to read. These exploits affect only tables where the attacker lacks full read access but has both INSERT and UPDATE privileges. Exploits bypass row level security policies and lack of SELECT privilege.  
  
[CVE-2017-7484] It was found that some selectivity estimation functions in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 did not check user privileges before providing information from pg\_statistic, possibly leaking information. An unprivileged attacker could use this flaw to steal some information from tables they are otherwise not allowed to access.  
  
[CVE-2017-7485] In PostgreSQL 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3, it was found that the PGREQUIRESSL environment variable was no longer enforcing a SSL/TLS connection to a PostgreSQL server. An active Man-in-the-Middle attacker could use this flaw to strip the SSL/TLS protection from a connection between a client and a server.  
  
[CVE-2017-7486] PostgreSQL versions 8.4 - 9.6 are vulnerable to information leak in pg\_user\_mappings view which discloses foreign server passwords to any user having USAGE privilege on the associated foreign server.  
  
[CVE-2017-7546] PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to incorrect authentication flaw allowing remote attackers to gain access to database accounts with an empty password.  
  
[CVE-2017-7547] PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers to retrieve passwords from the user mappings defined by the foreign server owners without actually having the privileges to do so.  
  
[CVE-2017-7548] PostgreSQL versions before 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers with no privileges on a large object to overwrite the entire contents of the object, resulting in a denial of service.  
  
[CVE-2018-1053] In postgresql 9.3.x before 9.3.21, 9.4.x before 9.4.16, 9.5.x before 9.5.11, 9.6.x before 9.6.7 and 10.x before 10.2, pg\_upgrade creates file in current working directory containing the output of `pg\_dumpall -g` under umask which was in effect when the user invoked pg\_upgrade, and not under 0077 which is normally used for other temporary files. This can allow an authenticated attacker to read or modify the one file, which may contain encrypted or unencrypted database passwords. The attack is infeasible if a directory mode blocks the attacker searching the current working directory or if the prevailing umask blocks the attacker opening the file.  
  
[CVE-2018-10915] "A vulnerability was found in libpq, the default PostgreSQL client library where libpq failed to properly reset its internal state between connections. If an affected version of libpq was used with ""host"" or ""hostaddr"" connection parameters from untrusted input, attackers could bypass client-side connection security features, obtain access to higher privileged connections or potentially cause other impact through SQL injection, by causing the PQescape() functions to malfunction. Postgresql versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 are affected."  
  
[CVE-2018-10925] "It was discovered that PostgreSQL versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 failed to properly check authorization on certain statements involved with ""INSERT ... ON CONFLICT DO UPDATE"". An attacker with ""CREATE TABLE"" privileges could exploit this to read arbitrary bytes server memory. If the attacker also had certain ""INSERT"" and limited ""UPDATE"" privileges to a particular table, they could exploit this to update other columns in the same table."  
  
[CVE-2018-1115] postgresql before versions 10.4, 9.6.9 is vulnerable in the adminpack extension, the pg\_catalog.pg\_logfile\_rotate() function doesn't follow the same ACLs than pg\_rorate\_logfile. If the adminpack is added to a database, an attacker able to connect to it could exploit this to force log rotation.  
  
[CVE-2018-7210] An issue was discovered in iDashboards 9.6b. It allows remote attackers to obtain sensitive information via a direct request for the idb/config?CMD=installLicense URI, as demonstrated by intranet IP addresses and names of guest accounts.  
  
[CVE-2019-10130] "A vulnerability was found in PostgreSQL versions 11.x up to excluding 11.3, 10.x up to excluding 10.8, 9.6.x up to, excluding 9.6.13, 9.5.x up to, excluding 9.5.17. PostgreSQL maintains column statistics for tables. Certain statistics, such as histograms and lists of most common values, contain values taken from the column. PostgreSQL does not evaluate row security policies before consulting those statistics during query planning  
[CVE-2019-10208] A flaw was discovered in postgresql versions 9.4.x before 9.4.24, 9.5.x before 9.5.19, 9.6.x before 9.6.15, 10.x before 10.10 and 11.x before 11.5 where arbitrary SQL statements can be executed given a suitable SECURITY DEFINER function. An attacker, with EXECUTE permission on the function, can execute arbitrary SQL as the owner of the function.  
  
[CVE-2019-10210] Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.  
  
[CVE-2019-10211] Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via bundled OpenSSL executing code from unprotected directory.  
  
[CVE-2019-25094] A vulnerability, which was classified as problematic, was found in innologi appointments Extension up to 2.0.5 on TYPO3. This affects an unknown part of the component Appointment Handler. The manipulation of the argument formfield leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.0.6 is able to address this issue. The identifier of the patch is 986d3cb34e5e086c6f04e061f600ffc5837abe7f. It is recommended to upgrade the affected component. The identifier VDB-217353 was assigned to this vulnerability.  
  
[CVE-2020-14350] It was found that some PostgreSQL extensions did not use search\_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.  
  
[CVE-2020-1720] "A flaw was found in PostgreSQL's ""ALTER ... DEPENDS ON EXTENSION"", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17."  
  
[CVE-2020-25694] A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.  
  
[CVE-2020-25695] A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.  
  
[CVE-2020-25696] A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If an interactive psql session uses \gset when querying a compromised server, the attacker can execute arbitrary code as the operating system account running psql. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.  
  
[CVE-2021-32027] A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.  
  
[CVE-2021-37665] TensorFlow is an end-to-end open source platform for machine learning. In affected versions due to incomplete validation in MKL implementation of requantization, an attacker can trigger undefined behavior via binding a reference to a null pointer or can access data outside the bounds of heap allocated arrays. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl\_requantization\_range\_per\_channel\_op.cc) does not validate the dimensions of the `input` tensor. A similar issue occurs in `MklRequantizePerChannelOp`. The [implementation](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl\_requantize\_per\_channel\_op.cc) does not perform full validation for all the input arguments. We have patched the issue in GitHub commit 9e62869465573cb2d9b5053f1fa02a81fce21d69 and in the Github commit 203214568f5bc237603dbab6e1fd389f1572f5c9. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.  
  
[CVE-2022-3952] A vulnerability has been found in ManyDesigns Portofino 5.3.2 and classified as problematic. Affected by this vulnerability is the function createTempDir of the file WarFileLauncher.java. The manipulation leads to creation of temporary file in directory with insecure permissions. Upgrading to version 5.3.3 is able to address this issue. The name of the patch is 94653cb357806c9cf24d8d294e6afea33f8f0775. It is recommended to upgrade the affected component. The identifier VDB-213457 was assigned to this vulnerability.  
  
[CVE-2012-1618] "Interaction error in the PostgreSQL JDBC driver before 8.2, when used with a PostgreSQL server with the ""standard\_conforming\_strings"" option enabled, such as the default configuration of PostgreSQL 9.1, does not properly escape unspecified JDBC statement parameters, which allows remote attackers to perform SQL injection attacks. NOTE: as of 20120330, it was claimed that the upstream developer planned to dispute this issue, but an official dispute has not been posted as of 20121005."  
  
[CVE-2014-0067] "The ""make check"" command for the test suites in PostgreSQL 9.3.3 and earlier does not properly invoke initdb to specify the authentication requirements for a database cluster to be used for the tests, which allows local users to gain privileges by leveraging access to this cluster."  
  
[CVE-2016-5424] "PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) "" (double quote), (2) \ (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation."  
  
  
  
Emptys

### Узел 127.0.0.37/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.69/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.2/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.38/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.70/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.3/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.39/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.71/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.4/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.40/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.72/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.5/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.41/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.73/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.6/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.42/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.74/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.43/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.7/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.75/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.44/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.8/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.76/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.45/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.9/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.77/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.46/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.10/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.78/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.47/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.11/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.79/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.12/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.48/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.80/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.13/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.49/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.81/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.14/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.50/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.82/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.15/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.51/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.83/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.16/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.52/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.84/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.53/24

Состояние: up

Количество открытых портов: 2

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |
| 53 | open | syn-ack | domain |  |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.  
  
  
  
Emptys

### Узел 127.0.0.17/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.85/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.54/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.18/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.86/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.55/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.19/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.87/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.56/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.20/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.88/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.57/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.21/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.89/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.58/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.22/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.90/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.23/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.59/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.91/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.24/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.60/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.92/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.25/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.61/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.93/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.26/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.62/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.94/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.27/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.63/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.95/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.28/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.29/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.30/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.96/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.128/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.97/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.31/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.129/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.98/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.99/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.130/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.131/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.160/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.161/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.132/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.162/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.133/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.134/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.163/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.135/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.164/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.100/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.101/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.102/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.103/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.104/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.136/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.165/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.105/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.137/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.166/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.106/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.167/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.138/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.107/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.168/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.139/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.108/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.169/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.140/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.109/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.170/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.141/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.110/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.171/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.142/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.111/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.172/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.173/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.143/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.144/24

Состояние: up

Количество открытых портов: 0

Общее количество CVE: 10

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |

#### Описание CVE:

### Узел 127.0.0.112/24

Состояние: up

Количество открытых портов: 1

Общее количество CVE: 12

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |
| 22 | open | syn-ack | ssh | [CVE-2021-36368] - Низкая [CVE-2023-28531] - Критичная [CVE-1999-0661] - Информация неизвестна [CVE-2007-4654] - Средняя [CVE-2010-4755] - Средняя [CVE-2016-20012] - Средняя [CVE-2019-16905] - Высокая [CVE-2020-12062] - Высокая [CVE-2020-14145] - Средняя [CVE-2020-15778] - Высокая [CVE-2021-28041] - Высокая [CVE-2021-41617] - Высокая |

#### Описание CVE:

update\_cve.csv:  
[CVE-2021-36368] "\*\* DISPUTED \*\* An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is ""this is not an authentication bypass, since nothing is being bypassed."""  
  
[CVE-2023-28531] ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.  
  
[CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.  
  
[CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.  
  
[CVE-2010-4755] The (1) remote\_glob function in sftp-glob.c and the (2) process\_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH\_FXP\_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.  
  
[CVE-2016-20012] \*\* DISPUTED \*\* OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.  
  
[CVE-2019-16905] OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.  
  
[CVE-2020-12062] "\*\* DISPUTED \*\* The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ""this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol"" and ""utimes does not fail under normal circumstances."""  
  
[CVE-2020-14145] The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.  
  
[CVE-2020-15778] "\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ""anomalous argument transfers"" because that could ""stand a great chance of breaking existing workflows."""  
  
[CVE-2021-28041] ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.  
  
[CVE-2021-41617] sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

### Узел 127.0.0.113/24

Состояние: up

Количество открытых портов: 0

Общее количество CVE: 6

#### Таблица информации о портах:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер порта | Состояние | Причина | Сервис | CVE |

#### Описание CVE: