# CA23-29

**Issued:** October 11, 2023
**Updated:** N/A
**Version:** 1.0
**Severity:** High
**Score:** CVSS 8.8
**Third Party Publication / CVE:** CVE-2023-38408 (https://nvd.nist.gov/vuln/detail/CVE-2023-38408)
**Note:** The score reflects the severity of the issue based on the specific implementation in CyberArk products, and therefore may differ from the original CVE score.
**Impact:** A remote unauthenticated threat actor could exploit this vulnerability in OpenSSH v7.7p1, on a server that is using SSH agent forwarding, to achieve remote code execution (RCE).

**Affected products and versions:**

| Product* | Version(s)** | Additional Information |
|---|---|---|
| Privileged Session Manager for SSH (PSM for SSH), Self-Hosted | Version 13.2 and earlier | All product subsets are affected |

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.
** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

**Resolution:**
Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm) in our online documentation.
If a patch isn't available for your installed version, or if you want to move to the latest available version, upgrade your component according to the upgrade version compatibility (https://docs.cyberark.com/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm#Upgradeversioncompatibility) docs.

| Installed version | Patch version | Download link | Documentation |
|---|---|---|---|
| PSM for SSH 13.2 (STS) and its patches prior to 13.2.4, or older versions | 13.2.4 | https://www.cyberark.com/CA23-29-13.2.4 (https://www.cyberark.com/CA23-29-13.2.4) or https://www.cyberark.com/CA23-29-13.2.4-RHEL8 (https://www.cyberark.com/CA23-29-13.2.4-RHEL8) | Upgrade PSM for SSH 13.2 (https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |
| PSM for SSH 13.0 (STS) and its patches prior to 13.0.4, or older versions | 13.0.4 | https://www.cyberark.com/CA23-29-13.0.4 (https://www.cyberark.com/CA23-29-13.0.4) or https://www.cyberark.com/CA23-29-13.0.4-RHEL8 (https://www.cyberark.com/CA23-29-13.0.4-RHEL8) | Upgrade PSM for SSH 13.0 (https://docs.cyberark.com/PAS/13.0/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |
| PSM for SSH 12.6 (LTS) and its patches prior to 12.6.10, or older versions | 12.6.10 | https://www.cyberark.com/CA23-29-12.6.10 (https://www.cyberark.com/CA23-29-12.6.10) or https://www.cyberark.com/CA23-29-12.6.10-RHEL8 (https://www.cyberark.com/CA23-29-12.6.10-RHEL8) | Upgrade PSM for SSH 12.6 (https://docs.cyberark.com/PAS/12.6/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |
| PSM for SSH 12.2 (LTS) and its patches prior to 12.2.15, or older versions | 12.2.15 | https://www.cyberark.com/CA23-29-12.2.15 (https://www.cyberark.com/CA23-29-12.2.15) or https://www.cyberark.com/CA23-29-12.2.15-RHEL8 (https://www.cyberark.com/CA23-29-12.2.15-RHEL8) | Upgrade PSM for SSH 12.2 (https://docs.cyberark.com/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |
| PSM for SSH 11.5 (LTS) and its patches prior to 11.5.19, or older versions | 11.5.19 | https://www.cyberark.com/CA23-29-11.5.19 (https://www.cyberark.com/CA23-29-11.5.19) | Upgrade PSM for SSH 11.5 (https://docs.cyberark.com/PAS/11.5/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |

**Temporary mitigation:**
There is no temporary mitigation available for this security bulletin.

**Exploited in the wild in a CyberArk environment:**
Not to the best of CyberArk's knowledge.

**Technical FAQ**
**Where can I see the changes done in newer versions?**
All release notes can be found here (https://docs.cyberark.com/PAS/Latest/en/Content/Release%20Notes/RN-ReleaseNotesIntro.htm).
For more technical information, please see the Technical FAQ (https://www.cyberark.com/ca23-29-faq).

**References:**
CyberArk End of Life Policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm)
CyberArk Security Vulnerability Management Policy (https://www.cyberark.com/cyberark-security-vulnerability-policy.pdf)
CyberArk Marketplace (https://cyberark-customers.force.com/mplace/s/)
CyberArk Online Documentation (https://docs.cyberark.com/Product-Doc/OnlineHelp/Portal/Content/Resources/_TopNav/cc_Portal.htm)

# CA23-30

**Issued:** October 11, 2023
**Updated:** N/A
**Version:** 1.0
**Severity:** High
**Score:** CVSS 7.5
**Third Party Publication / CVE:** N/A
**Impact:** A remote unauthenticated threat actor may exploit this vulnerability to perform a Denial of Service (DoS) attack.

**Affected products and versions:**

| Product* | Version(s)** | Additional Information |
|---|---|---|
| Privileged Session Manager for SSH (PSM for SSH), Self-Hosted | Version 12.2 and earlier | All product subsets are affected |

* This Security Bulletin applies only to the listed affected products. If this issue also affects another CyberArk product, it will be addressed in a separate Security Bulletin.
** Relates only to versions that are within their development life cycle. Refer to our End of Life policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm) for details.

**Resolution:**
Upgrade to a patch version from the table below by downloading the patch from the respective link and following the instructions (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager.htm) in our online documentation.
If a patch isn't available for your installed version, or if you want to move to the latest available version, upgrade your component according to the upgrade version compatibility (https://docs.cyberark.com/PAS/latest/en/Content/PAS%20INST/Considerations-before-Upgrading.htm#Upgradeversioncompatibility) docs.

| Installed version | Patch version | Download link | Documentation |
|---|---|---|---|
| PSM for SSH 12.2 (LTS) and its patches prior to 12.2.15, or older versions | 12.2.15 | https://www.cyberark.com/CA23-30-12.2.15 (https://www.cyberark.com/CA23-30-12.2.15) or https://www.cyberark.com/CA23-30-12.2.15-RHEL8 (https://www.cyberark.com/CA23-30-12.2.15-RHEL8) | Upgrade PSM for SSH 12.2 (https://docs.cyberark.com/PAS/12.2/en/Content/PAS%20INST/Upgrading-the-Privileged-Session-Manager-SSH-Proxy.htm) |

**Temporary mitigation:**
There is no temporary mitigation available for this security bulletin.

**Exploited in the wild in a CyberArk environment:**
Not to the best of CyberArk's knowledge.

**Technical FAQ**
**I am using PSM for SSH version 11.5 and there is no patch for this version, why?**
In line with CyberArk's End-of-Life policy (https://docs.cyberark.com/EOL/en/Content/End-Of-LifePolicy.htm), only versions within their Development Period receive patches. Since this security vulnerability was discovered after v11.5 reached its End of Development period, there is no patch for this version. Customers are recommended to upgrade to v12.2.15 or higher.
For more technical information, please see the Technical FAQ (https://www.cyberark.com/ca23-30-faq).

**References:**
CyberArk End of Life Policy (https://docs.cyberark.com/Product-Doc/OnlineHelp/EOL/en/Content/End-Of-LifePolicy.htm)
CyberArk Security Vulnerability Management Policy (https://www.cyberark.com/cyberark-security-vulnerability-policy.pdf)
CyberArk Marketplace (https://cyberark-customers.force.com/mplace/s/)
CyberArk Online Documentation (https://docs.cyberark.com/Product-Doc/OnlineHelp/Portal/Content/Resources/_TopNav/cc_Portal.htm)