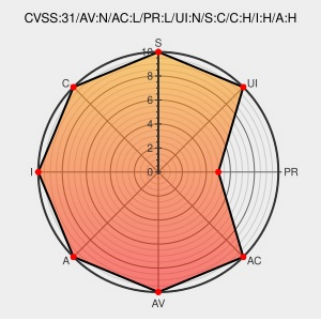
CVE-2018-18556

Published on: 12/17/2018 12:00:00 AM UTC

Last Modified on: 01/20/2023 03:28:00 PM UTC

CVE-2018-18556

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



Certain versions of Vyos from Vyos contain the following vulnerability:

A privilege escalation issue was discovered in VyOS 1.1.8. The default configuration also allows operator users to execute the pppd binary with elevated (sudo) permissions. Certain input parameters are not properly validated. A malicious operator user can run the binary with elevated permissions and leverage its improper input validation condition to spawn an attacker-controlled shell with root privileges.

CVE-2018-18556 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.9 - CRITICAL

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
VyOS restricted-shell Escape / Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159234/VyOS-restricted-shell-Escape-Privilege-Escalation.html
CVE-2018-18556 – VyOS Privilege escalation via sudo	Exploit	MISC blog.mirch.io/2018/11/05/cve-2018-18556-

pppd for operator users – Rich Mirch	Exploit Third Party Advisory blog.mirch.io text/html	vyos-privilege-escalation-via-sudo-pppd-for-operator-users/
The "operator" level is proved insecure and will be removed in the next releases	Exploit Vendor Advisory blog.vyos.io text/html	CONFIRM blog.vyos.io/the-operator-level-is-proved-insecure-and-will-be-removed-in-the-next-releases

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Vyos	Vyos	1.1.8	All	All	All
Operating System	Vyos	Vyos	1.1.8	All	All	All

cpe:2.3:o:vyos:vyos:1.1.8:*:*:*:*:*:*:*:

cpe:2.3:o:vyos:vyos:1.1.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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

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