

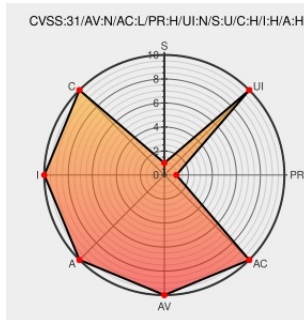


CVE-2018-9276

Published on: 07/02/2018 12:00:00 AM UTC

Last Modified on: 04/25/2023 03:41:00 PM UTC

CVE-2018-9276

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Prtg Network Monitor](#) from [Paessler](#) contain the following vulnerability:

An issue was discovered in PRTG Network Monitor before 18.2.39. An attacker who has access to the PRTG System Administrator web console with administrative privileges can exploit an OS command injection vulnerability (both on the server and on devices) by sending malformed parameters in sensor or notification management scenarios.

CVE-2018-9276 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	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
PRTG Network Monitor 18.2.38 - (Authenticated) Remote Code Execution - Windows webapps Exploit	Exploit Third Party Advisory VDB Entry	EXPLOIT-DB 46527

	www.exploit-db.com Proof of Concept text/html	
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	 BUGTRAQ 20180626 PRTG < 18.2.39 Command Injection
PRTG Network Monitor Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/161183/PRTG-Network-Monitor-Remote-Code-Execution.html
PRTG Command Injection ≈ Packet Storm	Exploit Mitigation Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/148334/PRTG-Command-Injection.html

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
Application	Paessler	Prtg Network Monitor	All	All	All	All
Application	Paessler Ag	Prtg Network Monitor	All	All	All	All
Application	Paessler Ag	Prtg Network Monitor	All	All	All	All
cpe:2.3:a:paessler:prtg_network_monitor:*:*:*:*:*:*:						
cpe:2.3:a:paessler_ag:prtg_network_monitor:*:*:*:*:*:*:						
cpe:2.3:a:paessler_ag:prtg_network_monitor:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

