NATIONAL
CSIRT CY

FortiWeb - Unauthenticated SQL injection in GUI

13/07/2025

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] in FortiWeb may allow an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.

Analysis

The attack can be extended further to remote code execution by embedding a SELECT ... INTO OUTFILE statement to write a malicious payload to a file in the underlying operating system by taking advantage of the fact that the query is run as the "mysql" user, and execute it via Python.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/89.html

Solutions

Version	Affected	Solution
FortiWeb 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiWeb 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
FortiWeb 7.2	7.2.0 through 7.2.10	Upgrade to 7.2.11 or above
FortiWeb 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.