NATIONAL CSIRT-CY

CVE-2024-55591

Authentication bypass in Node.js websocket module

14/1/2025

Executive Summary

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.

Analysis

The operations performed by the Threat Actor (TA) in the cases we observed were part or all of the below:

1. Creating an admin account on the device with random user name
2. Creating a Local user account on the device with random user name
3. Creating a user group or adding the above local user to an existing sslvpn user group
4. Adding/changing other settings (firewall policy, firewall address, ...)
5. Logging in the sslvpn with the above added local users to get a tunnel to the internal network.

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

Common Weakness Enumeration

https://www.cve.org/CVERecord?id=CVE-2024-55591

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2024-55591

Affected Systems and Solutions

Version	Affected	Solution
FortiOS 7.0	7.0.0 through 7.0.16	Upgrade to 7.0.17 or above
FortiProxy 7.2	7.2.0 through 7.2.12	Upgrade to 7.2.13 or above
FortiProxy 7.0	7.0.0 through 7.0.19	Upgrade to 7.0.20 or above

Appendix – Possible IOCs

Type	Description
Log Entry Following login activity log with random scrip and dstip	type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1733486785" user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin logged in successfully from jsconsole"
Log Entry Following admin creation log with seemingly randomly generated user name and source IP	type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="admin" ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin" cfgobj="vOcep" cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin vOcep"
IP address	45.55.158.47 [most used IP address]
IP address	87.249.138.47
IP address	155.133.4.175
IP address	37.19.196.65
IP address	149.22.94.37

The following IP addresses were mostly found used by attackers in above logs:
1.1.1.1
127.0.0.1
2.2.2.2
8.8.8.8
8.8.4.4

Admin or Local user created by the TA is randomly generated. e.g: Gujhmk, Ed8x4k, G0xgey, Pvnw81, Alg7c4, Ypda8a, Kmi8p4, 1a2n6t, 8ah1t6, M4ix9f, etc.

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.