

Denial of service
Remote Code Execution

Affected Products

FortiOS 5.6.0 to 5.6.10

FortiOS 5.4.0 to 5.4.12

FortiOS 5.2.0 to 5.2.14

FortiOS 6.0.0 to 6.0.4

.Branch lower than 5.2 not been assessed

,Vulnerable to vulnerabilities that could allow remote
,authenticated-validated code to run on the device
or read files from the device, including user credentials

[עדכון] FortiOS 5.4.1 to 5.4.10

FortiOS 5.6.0 to 5.6.8 [עדכון]

FortiOS 6.0.0 to 6.0.4

לאחר העדכון, מומלץ לבחון האפשרות לאתחול סיסמאות הגישה לכלל המשתמשים בצידוד ה-VPN,

בפרט אם בלוגים של הצידוד מופיעות פניות הכוללות את המחרוזת " ../.. "

מאחר ומכשיר פורטיגייט מגיע עם תעודות אבטחה SSL כברירת מחדל חתומה ע"י Fortinet גורם צד שלישי יכול לבצע התחזות לאותה תעודה כל עוד הוא מחזיק בתעודה אחרת שנחתמה ע"י פורטינט או גורם מאשר אמין אחר. הסיבה לכן היא כי תעודת ה-SSL המותקנת כברירת מחדל משתמשת במספר הסידורי של הנתב בתור שם השרת,

אך תוכנת ה- Forti client אינה מאמתת את שם השרת.

מומלץ להחליף את התעודה הדיגיטלית באופן ידני לתעודה שתונפק ע"י גורם מאשר מוסמך

אין להסתפק בעדכון לגרסאות המוזכרות בפרסומי המערך משנה שעברה, מאחר ומאז

החברה פרסמה עוד כ-20 עדכוני אבטחה לפגיעויות נוספות, בדרגות חומרה פגיעות המאפשרת מעקף של הזדהות חזקה CVE-2020-12812 שונות, כולל במקרים מסוימים

ניתן להיעזר בכלי הבא לזיהוי הגרסה העדכנית ביותר המתאימה למוצר 3. שברשותכם

[.https://docs.fortinet.com/upgrade-tool](https://docs.fortinet.com/upgrade-tool)

4. לאחר העדכון, מומלץ מאד לאתחל את סיסמאות הגישה של כלל המשתמשים בצידוד.

5. מומלץ להשתמש (Multi Factor Authentication) עבור גישה באמצעות בהזדהות חזקה VPN. לרשת הארגונית

1. <https://www.gov.il/he/departments/publications/reports/vpn-urgent-alert>
2. <https://www.gov.il/he/departments/publications/reports/vpn-urgent-alert-update>
3. <https://www.gov.il/he/departments/publications/reports/vpn-urgent-alert-3>
4. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379>
5. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12812>
6. <https://www.fortiguard.com/psirt/FG-IR-18-384>
7. <https://www.fortiguard.com/psirt/FG-IR-19-283>