مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerabilities in WatchGuard SSO Agent

Tracking #:432316334

Date:26-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed WatchGuard's has released security advisory concerning critical vulnerabilities affecting its SSO Agent.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE ID**: CVE-2024-6592, CVE-2024-6593
- **Severity**: Critical
- **CVSS Score**: 9.1
- CVE-2024-6593-An incorrect authorization vulnerability in WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows allows an attacker with network access to execute restricted management commands.
- CVE-2024-6592-An incorrect authorization vulnerability in the protocol communication between the WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows and the WatchGuard Single Sign-On Client on Windows and MacOS allows an attacker with network access to forge communications to affected components.
- An attacker that has already gained network access could exploit this vulnerability to retrieve authenticated usernames and group memberships from the Single Sign-On Agent or tamper with the agent configuration. This vulnerability cannot be used by an attacker to gain access to user credentials.
- Affected Products: Authentication Gateway: through 12.10.2; Windows Single Sign-On Client: through 12.7; MacOS Single Sign-On Client: through 12.5.4.
- **Fixed Versions:** None, Not yet Released

- **Workaround Recommendations:**
  - Implementing Windows Firewall rules to restrict TCP port 4116 network access to only allow connections from the Authentication Gateway (SSO Agent).
  - Restricting TCP port 4114 network access to the Authentication Gateway, allowing connections solely from the Firebox.
  - Utilizing Group Policy objects for adding firewall rules on Windows endpoints.

RECOMMENDATIONS:

- Organizations using affected products should implement recommended workarounds promptly and monitor for any updates from WatchGuard regarding patches or further guidance.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00014
- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00015