مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- SolarWinds

Tracking #:432316403

Date:17-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SolarWinds has released security patches to address multiple vulnerabilities affecting its Serv-U FTP Service, SolarWinds Platform, SolarWinds Web Help Desk products. If exploited, these vulnerabilities could lead to remote code execution and local privilege escalation.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **SolarWinds Web Help Desk Java Deserialization Remote Code Execution Vulnerability (CVE-2024-28988)**
   - **CVSS Score:** 9.8 Critical
   - SolarWinds Web Help Desk contains a critical Java Deserialization Remote Code Execution vulnerability. Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to the affected system and execute arbitrary code, potentially leading to significant consequences
2. **Serv-U FTP Service Directory Traversal Remote Code Execution Vulnerability (CVE-2024-45711)**
   - **CVSS Score:** 7.5 (High)
   - A directory traversal vulnerability exists in Serv-U FTP Service, allowing attackers to execute arbitrary code on the affected system. This vulnerability requires authentication but can be exploited by authenticated users with sufficient privileges.
3. **SolarWinds Platform Uncontrolled Search Path Element Local Privilege Escalation Vulnerability (CVE-2024-45710)**
   - **CVSS Score:** 7.8 (High)
   - A local privilege escalation vulnerability exists in SolarWinds Platform, allowing low-privileged users with local access to escalate their privileges. This vulnerability can be exploited by manipulating the search path element.
4. **SolarWinds Platform Edit Function Cross-Site Scripting Vulnerability (CVE-2024-45715)**
   - **CVSS Score:** 7.1 (High)
   - A cross-site scripting (XSS) vulnerability exists in SolarWinds Platform's edit function. This vulnerability could allow attackers to inject malicious code into web pages, potentially leading to unauthorized access or data theft.

Affected Versions:

- Serv-U 15.4.2 and previous versions
- SolarWinds Platform 2024.2.1 and all previous versions
- SolarWinds Web Help Desk 12.8.3 HF2 and all previous versions

Fixed Versions:

- Serv-U 15.5 or later
- SolarWinds Platform 2024.4 or later
- SolarWinds Web Help Desk 12.8.3 HF3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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.solarwinds.com/trust-center/security-advisories