FORTINET

OUTBREAK ALERTS

Sunhillo SureLine Command Injection Attack

Surveillance application actively targeted

https://www.sunhillo.com/fb011/

CVEs: CVE-2021-36380

The attack on Sunhillo SureLine identified as CVE-2021-36380 allows a malicious actor to exploit an unauthenticated OS Command Injection vulnerability. Once established, the attacker can gain command over the targeted system and potentially achieving full system compromise.

Background

The Sunhillo products handles the surveillance data distribution systems for the Federal Aviation Administration, US Military, civil aviation authorities, and national defense organizations.

Announced

The vulnerability exists in the Sureline software due to improper input validation in the "ipAddr" and "dnsAddr" parameters. That allows an attacker to manipulate the resulting command by injecting valid OS command input allowing the establishment of an interactive remote shell session.

Since October 2023, the FortiGuard has protection coverage against the vulnerability. Exploitation attempts has been intercepting attack attempts averaging at a thousand per day. Also, the Mirai malware are used as a payload for further infiltration. It is recommended to apply a firmware patch as recommended by the vendor to fully mitigate any risks.

Latest Developments

Apr 10, 2024: A video walkthrough has been added to the Outbreak Alert.

Apr 9, 2024: FortiGuard published an Outbreak Alert for the Sunhillo SureLine Command Injection Attack.

Mar 5, 2024: CISA has added CVE-2021-36380 to the Known Exploited Vulnerabilities catalog.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Oct 30, 2023: Fortinet published an IPS signatures to protect its customers from attack attempt.

Oct 09, 2023: FortiGuard Labs team observed that the IZLH9 Mirai-based DDoS campaign targeted Sunhillo SureLine and released a detailed analysis.
https://www.fortinet.com/blog/threat-research/v1zlh9-campaign-enhances-arsenal-with-scores-of-exploits

July 22, 2021: Sunhillo published the security bulletin and a patch notice.
https://www.sunhillo.com/fb011/

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

AV

Detects and blocks known malware related to the Sunhillo Sureline Attack (CVE-2021-36380)

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 92.03216	*DB 92.03216*	*DB 92.03216*	*DB 92.03216*	*DB 92.03216*	*DB 92.03216*	*DB 92.03216*

FortiADC	FortiProxy
DB 92.03216	*DB 92.03216*

AV (Pre-filter)

Detects and blocks known malware related to the Sunhillo Sureline Attack (CVE-2021-36380)

FortiEDR	FortiSandbox	FortiNDR
DB 92.03216	*DB 92.03216*	*DB 92.03216*

- **Exploitation**

IPS

Detects and blocks attack attempts targeting the Sunhillo Sureline vulnerability (CVE-2021-36380)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 26.684	*DB 26.684*	*DB 26.684*	*DB 26.684*	*DB 26.684*

Web App Security

Detects and blocks attack attempts targeting the Sunhillo Sureline vulnerability (CVE-2021-36380)

FortiWeb
DB 0.00374

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer	FortiSIEM	FortiSOAR
DB 2.00040	*v607*	*v7.4+*

Threat Hunting

FortiAnalyzer

RESPOND

Develop containment techniques to mitigate impacts of security events:

Playbook

undefined

FortiSOAR	FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

Threat Hunting

undefined

FortiNDR Cloud

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training	Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Additional Resources

Security Affairs
https://securityaffairs.com/160081/security/cisa-android-pixel-sunhillo-sureline-bugs-known-exploited-vulnerabilities-catalog.html

Data breach Today
https://www.databreachtoday.com/patch-issued-for-flaw-in-sunhillo-sureline-surveillance-app-a-17176

Learn more about FortiGuard Outbreak Alerts

FORTINET