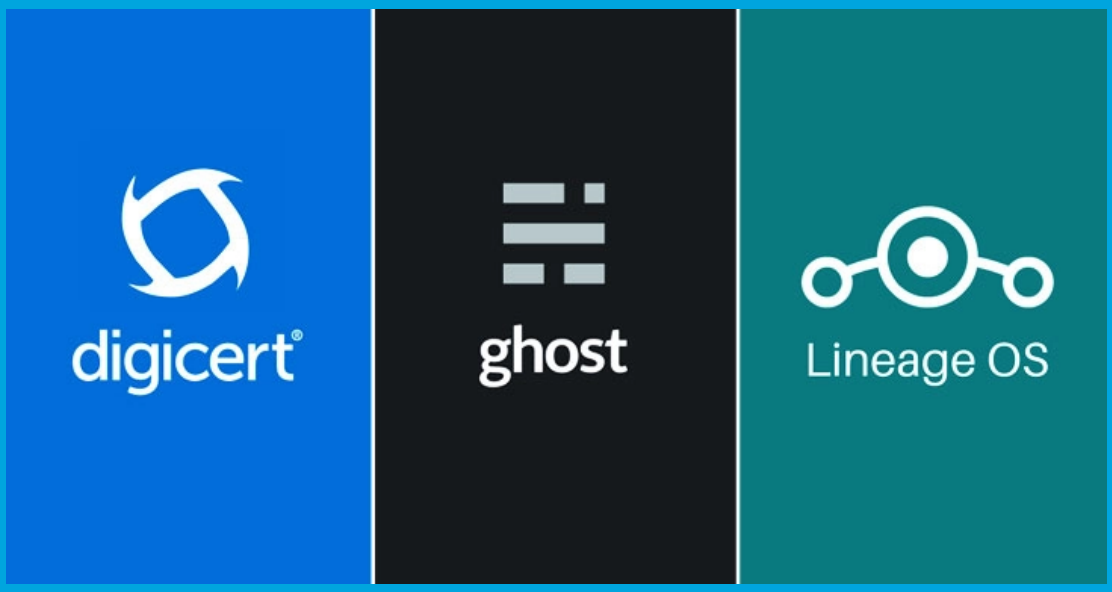
Security Newsletter

11 May 2020

Subscribe to this newsletter

Hackers Breach LineageOS, Ghost, DigiCert Servers Using SaltStack Vulnerability



Days after cybersecurity researchers sounded the alarm over two critical vulnerabilities in the SaltStack configuration framework, a hacking campaign has already begun exploiting the flaws to breach servers of LineageOS, Ghost, and DigiCert. Tracked as CVE-2020-11651 and CVE-2020-11652, the disclosed flaws could allow an adversary to execute arbitrary code on remote servers deployed in data centers and cloud environments. The issues were fixed by SaltStack in a release published on April 29th.

Salt versions before 3000.2 and 2019.2.4 are vulnerable to CVE-2020-11651 and CVE-2020-11652. F-Secure disclosed the two vulnerabilities last week saying that “any competent hacker” would need less than 24 hours to develop a 100% reliable exploit. These organizations above are just a few examples of victims of the two Salt vulnerabilities published by F-Secure. Coin mining seems to be the main goal of the threat actor but more insidious payloads could be used instead.

With F-Secure's alert revealing more than 6,000 Salt vulnerable servers that can be exploited via this vulnerability, if left unpatched, companies are advised to update the Salt software packages to the latest version to resolve the flaws.

Read More on TheHackerNews

Even More on BleepingComputer

More #News

- Search provider Algolia discloses security incident due to Salt vulnerability
- Apple and Google to prevent contact tracing apps from tracking your location
- Hacker sells 22 million Unacademy user records after data breach
- Large scale Snake Ransomware campaign targets healthcare, more
- GoDaddy – “unauthorized individual” had access to login info

- Microsoft launches IoT-focused bounty program with $100K awards
- Cisco Webex phishing uses fake cert errors to steal credentials
- Aria-body: This Asia-Pacific Cyber Espionage Campaign Went Undetected for 5 Years
- Credit card skimmer caught hiding behind website favico
- Microsoft: 150 million people are using passwordless logins each month
- Hacker gains access to a small number of Microsoft's private GitHub repos
- Firefox's Private Relay service tests anonymous email alias feature
- Office 365 to stop data theft by disabling external forwarding
- Forget Whitelists and Blacklists: Go for 'Allow' or 'Deny'
- Denmark, Sweden, Germany, the Netherlands and France SIGINT Alliance
- Research Project: Malware Jumps Air-Gapped Devices by Turning Power-Supplies into Speakers
- ILOVEYOU: The Love Bug virus 20 years on – could it happen again?
- Nintendo Source Code for N64, Wii and GameCube Leaked
- CAM4 adult cam site exposes 11 million emails, private chats

#Patch Time!

- SaltStack CVE-2020-11651 and CVE-2020-11652 Attack
- Microsoft releases May Office updates with fixes for auth issues
- Firefox 76.0 released with critical security patches – update now
- Critical Citrix ShareFile bugs could give access to private files
- Critical WordPress plugin bug lets hackers take over 1M sites
- Cisco Patches High Severity Vulnerabilities in Security Products
- TP-Link Patches Multiple Vulnerabilities in NC Cloud Cameras
- Authentication bypass in FortiMail and FortiVoiceEntreprise
- Fixing SQL injection vulnerability and malicious code execution in XG Firewall/SFOS
- BIG-IQ Grafana vulnerability CVE-2020-5868

#Tech and #Tools

- Csper's Content Security Policy Journey
- The battle against ransomware: Lessons from the front lines
- Moving laterally between Azure AD joined machines
- AirIAM: Least privilege AWS IAM Terraformer
- Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents
- Splunk ES/Crowdstrike Threat Hunting Searches
- Bypass SSL Pinning on iOS 13 with FRIDA
- FalconZero v1.0 - a stealthy Windows Loader to deliver shellcode undetected
- Introduction to GCP Privilege Escalation
- Intro to GCP Privilege Escalation (Continued)
- YAS: Yet Another Sniffer

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us