kindred

Security Newsletter

28 Jun 2021

Subscribe to this newsletter

SolarWinds Hackers Breach Microsoft Customer Support to Target its Customers

In yet another sign that the Russian hackers who breached SolarWinds network monitoring software to compromise a slew of entities never really went away, Microsoft said the threat actor behind the malicious cyber activities used password spraying and brute-force attacks in an attempt to guess passwords and gain access to its customer accounts.

"This recent activity was mostly unsuccessful, and the majority of targets were not successfully compromised – we are aware of three compromised entities to date," the tech giant's Threat Intelligence Center said Friday. "All customers that were compromised or targeted are being contacted through our nation-state notification process."

Read More on The Hacker News

Even More on Microsoft's blog

More #News

- Hackers Use Fake Call Center to Trick Victims Into Installing Ransomware
- Antivirus creator John McAfee reportedly found dead in prison cell
- FIN7 Supervisor Gets 7-Year Jail Term for Stealing Millions of Credit Cards
- Microsoft admits to signing rootkit malware in supply-chain fiasco
- RIP: Internet Explorer will be disabled in Windows 11
- How Cyber Sleuths Cracked an ATM Shimmer Gang
- Amazon launching global competition to find and fix 1 million software bugs
- Google rolls out a unified security vulnerability schema for open-source software
- Microsoft's security tool can now spot rogue devices on your network
- Average time to fix critical cybersecurity vulnerabilities is 205 days: report

#Breach Log

- Nobelium hackers accessed Microsoft customer support tools
- Mercedes-Benz data breach exposes SSNs, credit card numbers
- WD My Book NAS devices are being remotely wiped clean worldwide
- Healthcare giant Grupo Fleury hit by REvil ransomware attack
- Tulsa warns of data breach after Conti ransomware leaks police citations
- ADATA suffers 700 GB data leak in Ragnar Locker ransomware attack
- Data leak marketplace pressures victims by emailing competitors

#Patch Time!

- Cisco ASA vulnerability actively exploited after exploit released
- Dell SupportAssist bugs put over 30 million PCs at risk
- VMware fixes authentication bypass in Carbon Black App Control
- Zephyr RTOS fixes Bluetooth bugs that may lead to code execution
- Tor Browser fixes vulnerability that tracks you using installed apps
- Zyxel Firewalls and VPNs Under Active Cyberattack

#Tech and #Tools

- SonicWall bug affecting 800K firewalls was only partially fixed
- Malicious PyPI packages hijack dev devices to mine cryptocurrency
- A supply-chain breach: Taking over an Atlassian account
- NFC flaws let researchers hack an ATM by waving a phone
- Crackonosh: A New Malware Distributed in Cracked Software
- Wardialing Finnish Freephones
- Linux marketplaces vulnerable to RCE and supply chain attacks
- AD CS relay attack - practical guide
- D3FEND Matrix | MITRE D3FEND

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

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

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