kindred

Security Newsletter

12 Jul 2021

Subscribe to this newsletter

Kaseya Left Customer Portal Vulnerable to 2015 Flaw in its Own Software

Last week cybercriminals deployed ransomware to 1,500 organizations, including many that provide IT security and technical support to other companies. The attackers exploited a vulnerability in software from Kaseya, a Miami-based company whose products help system administrators manage large networks remotely. Now it appears Kaseya's customer service portal was left vulnerable until last week to a data-leaking security flaw that was first identified in the same software six years ago.

On July 3, the REvil ransomware affiliate program began using a zero-day security hole (CVE-2021-30116) to deploy ransomware to hundreds of IT management companies running Kaseya's remote management software — known as the Kaseya Virtual System Administrator (VSA).

Also on July 3, security incident response firm Mandiant notified Kaseya that their billing and customer support site —portal.kaseya.net — was vulnerable to CVE-2015-2862, a "directory traversal" vulnerability in Kaseya VSA that allows remote users to read any files on the server using nothing more than a Web browser.

Read More on Krebs on Security

Even More on Ars Technica

Robbing the Xbox vault: Inside a $10 million gift card cheat

The Xbox gift card came with a string of 25 letters and numbers. The digits, known as a 5x5 code, were sent in an email, but they were no different from the numbers and letters etched onto the gift cards hanging off tall racks near the checkout aisle at CVS or Target, arrayed in a Rubik’s Cube of colors.

The cards themselves, of course, are worthless, but each 5x5 code corresponds to a dollar amount. In this case the code, DD9J9-MXXXC-3Y6XD-3QH2C-PWDWZ, was worth $15 toward the purchase of anything that Microsoft sold online. Volodymyr Kvashuk received the $15 code a few weeks before Christmas, in 2017, among a batch of 20 others worth $300 altogether.

Then Kvashuk found a bug that would change his life, a flaw so stupidly obvious that he couldn’t bring himself to report it to his managers. He noticed that whenever he tested purchases of gift cards, the Microsoft Store dispensed real 5x5 codes. It dawned on him: He could generate virtually unlimited codes, all for free.

Read More on Bloomberg

More #News

- Kaseya Rules Out Supply-Chain Attack; Says VSA 0-Day Hit Its Customers Directly
- Dozens of Vulnerable NuGet Packages Allow Attackers to Target .NET Platform
- Experts Uncover Malware Attacks Targeting Corporate Networks in Latin America
- New SaaS Security Report Dives into the Concerns and Plans of CISOs in 2021
- Biden asks Putin to crack down on Russian-based ransomware gangs
- Kaseya warns of phishing campaign pushing fake security updates

- Mozilla Firefox to roll out DNS over HTTPS for Canadian users
- Tens of thousands scammed using fake Android cryptomining apps
- Ransomware as a service: negotiators between hackers and victims are now in high demand
- Spike in “Chain Gang” Destructive Attacks on ATMs
- How to prevent ransomware attacks with a zero-trust security model
- Vulnerability in the Kaspersky Password Manager

#Breach Log

- REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom
- Hackers Scrape 90,000 GETTR User Emails, Surprising No One
- Mint Mobile hit by a data breach after numbers ported, data accessed
- Insurance giant CNA reports data breach after ransomware attack
- Morgan Stanley reports data breach after vendor Accellion hack

#Patch Time!

- Microsoft Issues Emergency Patch for Critical Windows PrintNightmare Vulnerability
- Interpol Arrests Moroccan Hacker Engaged in Nefarious Cyber Activities
- Microsoft's Emergency Patch Fails to Fully Fix PrintNightmare RCE Vulnerability
- How to Mitigate Microsoft Print Spooler Vulnerability – PrintNightmare
- Critical Flaws Reported in Sage X3 Enterprise Management Software
- Critical Flaws Reported in Philips Vue PACS Medical Imaging Systems
- Kaseya Releases Patches for Flaws Exploited in Widespread Ransomware Attack
- QNAP fixes critical bug in NAS backup, disaster recovery app

#Tech and #Tools

- Hackers Use New Trick to Disable Macro Security Warnings in Malicious Office Files
- Microsoft 365 to let SecOps lock hacked Active Directory accounts
- Account Takeover Protection and WAF mitigations to help stop Global Brute Force Campaigns
- Kaspersky Password Manager: All your passwords are belong to us
- Conti Unpacked | Understanding Ransomware Development As a Response to Detection
- Sneaky Malware Reconfigures Hive OS Wallet for Profit
- Microsoft Teams user enumeration
- Risk Assessment of GitHub Copilot

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