

NOW Live: Attack Surface Management Summit / Virtual Event - 11AM ET - Login Now



ATTACK SURFACE MANAGEMENT SUMMIT
WEDNESDAY, FEBRUARY 22, 2023

Malware & Threats ▾ Security Operations ▾ Security Architecture ▾
Risk Management ▾ CISO Strategy ▾ ICS/OT ▾ Funding/M&A ▾

REGISTER NOW

Virtual Event

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
www.securitysummits.com

CYBERCRIME

R1Soft Server Backup Manager Vulnerability Exploited to Deploy Backdoor

Hackers have been exploiting a vulnerability tracked as CVE-2022-36537 to hack hundreds of R1Soft servers.



By [Eduard Kovacs](#)
February 22, 2023



A vulnerability discovered last year in ConnectWise's R1Soft Server Backup Manager software has been exploited to

TRENDING

- 1 **AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm**
- 2 **Apple Updates Advisories as Security Firm Discloses New Class of Vulnerabilities**

deploy backdoors on hundreds of servers.

In late October 2022, ConnectWise informed customers that [a critical vulnerability](#) patched in Recover and R1Soft Server Backup Manager products that could allow an attacker to execute arbitrary code or directly access confidential data.

The vendor warned at the time that the flaw was at high risk of being exploited in the wild and urged users to patch their installations as soon as possible.

A few days later, managed endpoint detection and response (EDR) firm Huntress explained that this was actually an authentication bypass and sensitive file leak vulnerability affecting the ZK Java framework used by the R1Soft software. The flaw in ZK is tracked as CVE-2022-36537 and it was patched in May 2022.

Huntress researchers demonstrated at the time how an attacker could bypass authentication and upload a backdoored JDBC database driver to achieve arbitrary code execution, and push a piece of ransomware to all downstream

- 3 VMware Plugs Critical Carbon Black App Control Flaw**
- 4 HardBit Ransomware Offers to Set Ransom Based on Victim's Cyberinsurance**
- 5 Fortinet Patches Critical Code Execution Vulnerabilities in FortiNAC, FortiWeb**
- 6 Atlassian Investigating Security Breach After Hackers Leak Data**
- 7 CISA Warns of Two Mitel Vulnerabilities Exploited in Wild**
- 8 SolarWinds Announces Upcoming Patches for High-Severity Vulnerabilities**

endpoints managed by the software.

The security firm warned that there had been nearly 5,000 internet-exposed R1Soft servers at the time and hackers could exploit the vulnerability to push ransomware to these systems.

During a recent incident response case, cybersecurity company Fox-IT found evidence that the R1Soft vulnerability had been exploited to gain initial access to a server. The attackers then deployed a malicious database driver that gave them backdoor access.

An analysis by Fox-IT showed that the vulnerability has been [exploited in the wild](#) since late November 2022. On January 9, Fox-IT identified 286 backdoored servers, mainly in the United States and South Korea. As of February 20, the number dropped to 146 backdoored servers.

“With the help of fingerprinting, we have identified multiple compromised hosting providers globally,” Fox-IT said in a blog post on Wednesday.

Daily Briefing Newsletter

Subscribe to the SecurityWeek Email Briefing to stay informed on the latest threats, trends, and technology, along with insightful columns from industry experts.

Subscribe

Webinar: Building Sustainable OT Cybersecurity Programs

🕒 Thursday, February 23, 2023

Join this webinar to gain clear advice on the people, process and technology considerations that must be made at every stage of an OT security program’s lifecycle.

Register

Webinar: Entering the Cloud Native Security Era

🕒 Thursday, March 02, 2023

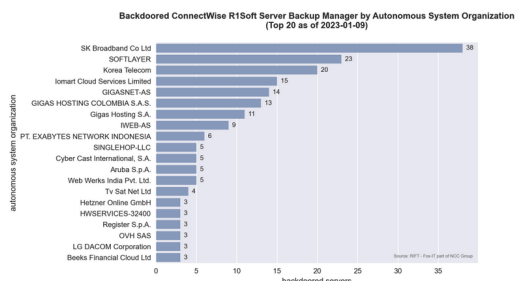
This presentation will provide an overview of the security risks associated with SaaS, best practices for mitigating these risks and protecting data, and discuss the importance of regularly reviewing and updating SaaS security practices to ensure ongoing protection of data.

Register

EXPERT INSIGHTS

Enterprise Blind Spots and Obsolete Tools – Security Teams Must Evolve

The conventional tools we rely on to defend corporate networks are creating gaps in



In the attacks observed by the company, the attackers exfiltrated files from compromised systems, including VPN configuration files, IT admin information, and sensitive documents.

Fox-IT has released indicators of compromise (IoCs) that can help organizations determine whether their systems have been hacked through exploitation of CVE-2022-36537.

Related: [CISA Warns of Two Mitel Vulnerabilities Exploited in Wild](#)

Related: [Surge in ESXiArgs Ransomware Attacks as Questions Linger Over Exploited Vulnerability](#)

Related: [Fortinet Patches Critical Code Execution Vulnerabilities in FortiNAC, FortiWeb](#)



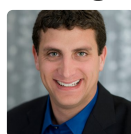
network visibility and in our capabilities to secure them. (Matt Wilson)

Application Security Protection for the Masses



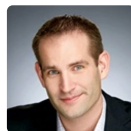
While there are many routes to application security, bundles that allow security teams to quickly and easily secure applications and affect security posture in a self-service manner are becoming increasingly popular. (Joshua Goldfarb)

Dealing With the Carcinization of Security



Varied viewpoints as related security concepts take on similar traits create substantial confusion among security teams trying to evaluate and purchase security technologies. (Marc Solomon)

Stop, Collaborate and Listen: Disrupting Cybercrime Networks Requires Private-Public Cooperation



No one combatting cybercrime knows everything, but everyone in the battle has some intelligence to contribute to the larger knowledge base. (Derek Manky)

How the Atomized Network Changed Enterprise Protection



Our networks have become atomized which, for starters, means they're highly dispersed. Not just in terms of the infrastructure – legacy, on-premises, hybrid, multi-cloud, and edge. (Matt Wilson)

WRITTEN BY

Eduard Kovacs

Eduard Kovacs
(@EduardKova)