Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

February 01, 2022

Alert Number
I-020122-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Scammers Exploit Security Weaknesses on Job Recruitment Websites to Impersonate Legitimate Businesses, Threatening Company Reputation and Defrauding Job Seekers

The FBI warns that malicious actors or 'scammers' continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to trick applicants into providing personal information or money. These scammers lend credibility to their scheme by using legitimate information to imitate businesses, threatening reputational harm for the business and financial loss for the job seeker.

Since early 2019, the average reported loss from this scheme is nearly $3,000 per victim, and many victims have also reported that the scheme negatively affected their credit scores.

FBI IC3

February 2022

security.org

March 2021

Account Takeover Fraud: A Consumer's Guide to Protecting Yourself

By Aliza Vigderman | Published March 17, 2021

Account takeover fraud is a type of cybercrime or identity theft where a malicious third-party gains access to (or "takes over") an online account, such as an e-mail address, bank account, or social media profile. In fact, our research shows it's happened to about 1 in 5 adults. In this guide, we break down exactly what account takeover is, how it happens, and most importantly, how to prevent it. Account takeover is often abbreviated as ATO or called account fraud.

Confluence Security Advisory 2022-06-02

Confluence Server and Data Center - CVE-2022-26134 - Critical severity unauthenticated remote code execution vulnerability

Still need help

The Atlassian Co
here for you.

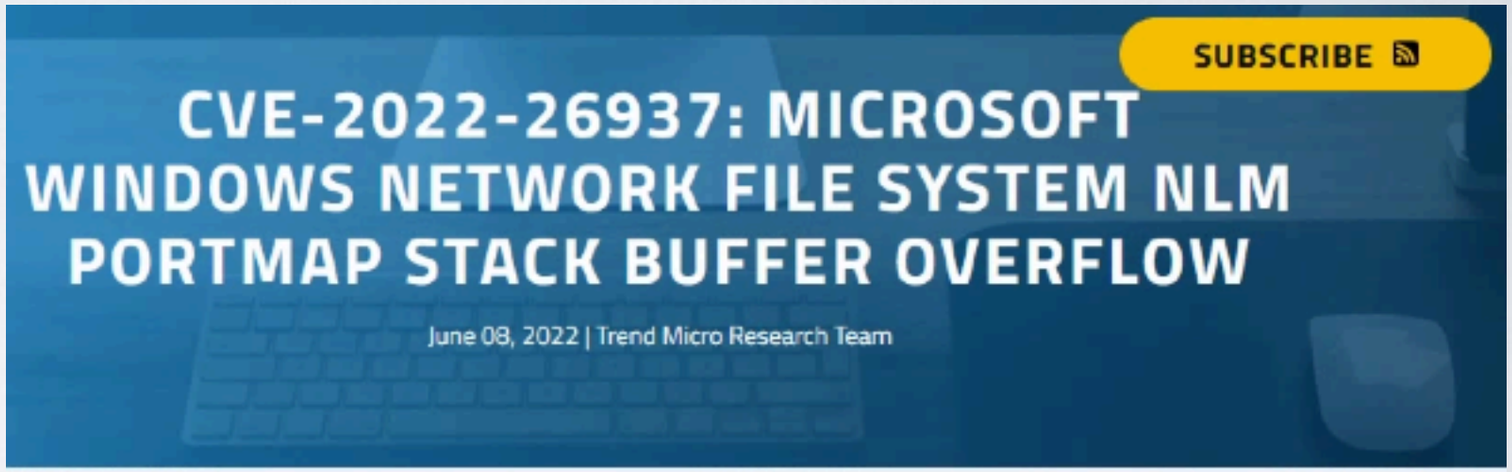
Ask the comm

Atlassian Advisories

June 2022

Zero Day Initiative

June 2022



Security advisory - ADAudit Plus Unauthenticated Remote Code Execution Vulnerability

CVEID: CVE-2022-28219

Severity: Critical

Affected Software Version(s): All ADAudit Plus builds below 7060 [How to find your build number]

Fixed Version(s): Build 7060

Fixed on: March 30, 2022

Details: ManageEngine ADAudit Plus had some vulnerable API endpoints that allowed an unauthenticated attacker to exploit XML External Entities (XXE), Java deserialization and path traversal vulnerabilities. The chain could be leveraged to perform unauthenticated remote code execution. This issue has been fixed.

Impact: An unauthenticated attacker would be able to remotely execute an arbitrary code in the ADAudit Plus server.

In this excerpt of a Trend Micro Vulnerability Research Service vulnerability report, Guy Lederfein and Jason McFadyen of the Trend Micro Research Team detail a recently patched code execution vulnerability in the Microsoft Windows operating system. The bug was originally discovered and reported to Microsoft by Yuki Chen. A stack buffer overflow vulnerability exists in Windows Network File System. A remote attacker can exploit this vulnerability by sending specially crafted RPC packets to a server, resulting in code execution in the context of SYSTEM. The following is a

ManageEngine Advisories

June 2022