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.

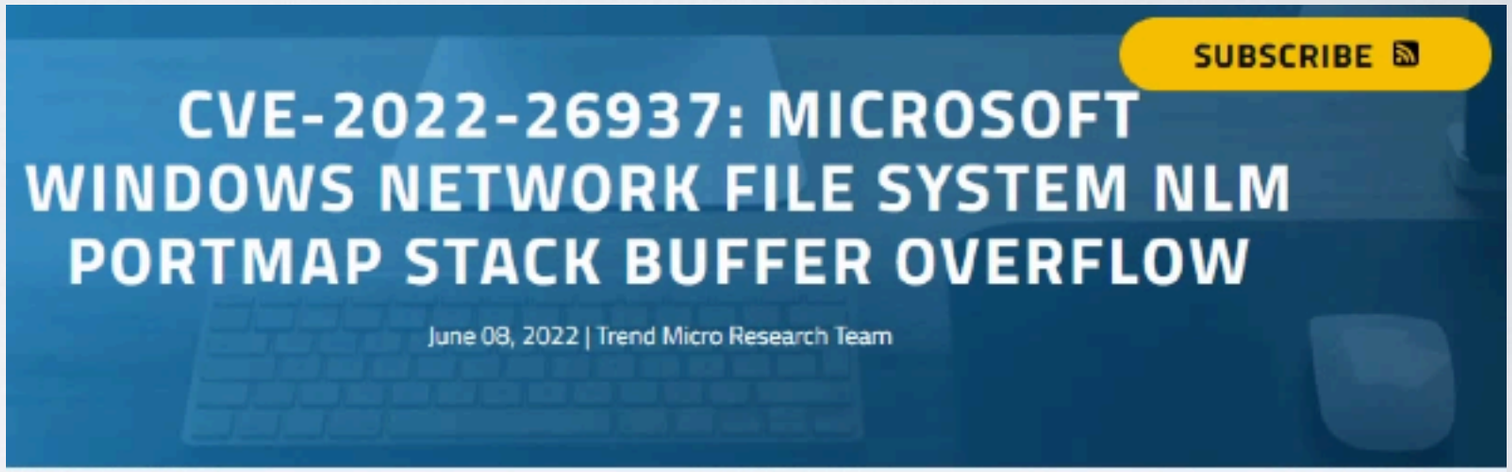
Ask the comm

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.

ManageEngine Advisories

June 2022

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

Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen

By Sergiu Gatlan — August 10, 2022 — 04:05 PM — 1

August 14th, 2022 update below. This post was originally published on August 10th.

Cisco confirmed today that the Yanluowang ransomware group breached its corporate network in late
the actor tried to extort them under the threat of leaking stolen files online.

The company revealed that the attackers could only harvest and steal non-sensitive data from a Box fo
a compromised employee's account.

Bleeping Computer

August 2022

Bleeping Computer

June 2022

Conti ransomware hacking spree breaches over 40 orgs in a month

By Ionut Ilascu — June 23, 2022 — 06:05 AM — 0

The Conti cybercrime syndicate runs one of the most aggressive ransomware operations and has grown highly organized, to the point that affiliates were able to hack more than 40 companies in a little over a month.

Security researchers codenamed the hacking campaign ARMattack and described it as being one of the group's "most productive" and "extremely effective."