

S T O R M ⚡ W A T C H

DATELINE : 2023-10-10



GREYNOISE
LABS

Microsoft Digital Defense Report

How can we protect against 99% of attacks?

While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

- 1 Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
- 2 Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
 - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
 - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.

– Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.

- 3 Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
- 4 Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
- 5 Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.¹



Enable multifactor authentication (MFA)



Apply Zero Trust principles



Use extended detection and response (XDR) and antimalware



Keep up to date



Protect data

Outlier attacks on the bell curve make up just 1%



GREYNOISE LABS

CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server

Summary of Vulnerability

Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances.

Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

⚠️ CVSS 10: URGENT ACTION REQUIRED

1. Upgrade your instance
2. Conduct comprehensive threat detection

Publicly accessible Confluence Data Center and Server versions as listed below are at critical risk and require immediate attention. See 'What You Need to Do' for detailed instructions.

Affected Versions

The Confluence Data Center and Server versions listed below are affected by this vulnerability. Customers using these versions should [upgrade your instance](#) as soon as possible.

Versions prior to 8.0.0 are not affected by this vulnerability.

Product	Affected Versions
Confluence Data Center and Confluence Server	<ul style="list-style-type: none"> • 8.0.0 • 8.0.1 • 8.0.2 • 8.0.3 • 8.0.4 • 8.1.0 • 8.1.1 • 8.1.3 • 8.1.4 • 8.2.0 • 8.2.1 • 8.2.2 • 8.2.3 • 8.3.0 • 8.3.1 • 8.3.2 • 8.4.0 • 8.4.1 • 8.4.2 • 8.5.0 • 8.5.1



Cisco Emergency Responder Static Credentials Vulnerability



Advisory ID:	cisco-sa-cer-priv-esc-B9t3hqk9	CVE-2023-20101	Download CSAF
First Published:	2023 October 4 16:00 GMT		Download CVRF
Version 1.0:	Final		Email
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCwh34565		
CVSS Score:	Base 9.8		

Summary

A vulnerability in Cisco Emergency Responder could allow an unauthenticated, remote attacker to log in to an affected device using the *root* account, which has default, static credentials that cannot be changed or deleted.

This vulnerability is due to the presence of static user credentials for the *root* account that are typically reserved for use during development. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and execute arbitrary commands as the *root* user.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.



Clorox, wipes?

Clorox warns of quarterly loss related to August cyberattack, production delays

The company is bracing for what could be an extended financial impact from the attack, which is reportedly linked to the Scattered Spider threat group.

Published Oct. 5, 2023



David Jones
Reporter



Clorox counting on streamlined operating model and \$500 million tech modernization to bounce back from post-pandemic slump. Justin Sullivan via Getty Images

Clorox said organic sales during the quarter, which ended September 30, are now expected to fall between 21% and 26% year over year, a contrast to the company's prior estimates of mid single-digit growth.



GREYNOISE
LABS

The International Committee of the Red Cross (ICRC) has, for the first time, published rules of engagement for civilian hackers involved in conflicts.

Based on international humanitarian law, the rules are:

1. Do not direct cyber-attacks against civilian objects
2. Do not use malware or other tools or techniques that spread automatically and damage military objectives and civilian objects indiscriminately
3. When planning a cyber-attack against a military objective, do everything feasible to avoid or minimise the effects your operation may have on civilians
4. Do not conduct any cyber-operation against medical and humanitarian facilities
5. Do not conduct any cyber-attack against objects indispensable to the survival of the population or that can release dangerous forces
6. Do not make threats of violence to spread terror among the civilian population
7. Do not incite violations of international humanitarian law
8. Comply with these rules even if the enemy does not



NSA, CISA Red and Blue Teams Share Top Ten Cyber Security Misconfigurations

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

This Week in KEV (TWiK?)

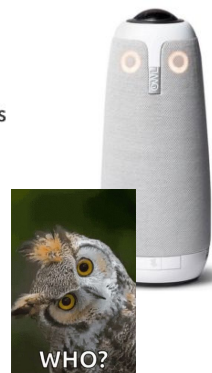
Added:

Apple	CVE-2023-42824
Atlassian	CVE-2023-22515
Progress	CVE-2023-40044
JetBrains	CVE-2023-42793
Microsoft	CVE-2023-28229

Removed:

CISA is continually collaborating with partners across government and the private sector. As a result of this collaboration, CISA has concluded that there is insufficient evidence to keep the following five CVEs in the catalog and has removed them:

- [CVE-2022-31459](#) Owl Labs Meeting Owl Inadequate Encryption Strength Vulnerability
- [CVE-2022-31460](#) Meeting Owl Pro and Whiteboard Owl Hard-Coded Credentials Vulnerability
- [CVE-2022-31461](#) Owl Labs Meeting Owl Missing Authentication for Critical Function Vulnerability
- [CVE-2022-31462](#) Owl Labs Meeting Owl Use of Hard-coded Credentials Vulnerability
- [CVE-2022-31463](#) Owl Labs Meeting Owl Improper Authentication Vulnerability



GREYNOISE
LABS

Reminder: curl release (8.4.0) Tomorrow



bagder

last week

Maintainer

edited



We are cutting the release cycle short and will release curl 8.4.0 on **October 11**, including fixes for a severity HIGH CVE and one severity LOW. The one rated HIGH is probably the worst curl security flaw in a long time.

The new version and details about the two CVEs will be published around 06:00 UTC on the release day.

- CVE-2023-38545: severity HIGH (affects both libcurl and the curl tool)
- CVE-2023-38546: severity LOW (affects libcurl only, not the tool)

There is no API nor ABI change in the coming curl release.

I cannot disclose any information about which version range that is affected, as that would help identify the problem (area) with a very high accuracy so I cannot do that ahead of time. The "last several years" of versions is as specific as I can get.

We have notified the [distros mailing list](#) allowing the member distributions to prepare patches. (No one else gets details about these problems before October 11 without a support contract and a good reason.)

Now you know. Plan accordingly.


↑ 290 😊 216 🤔 18 🍷 2 😬 30 ❤️ 62 🚀 95 🗨️ 161

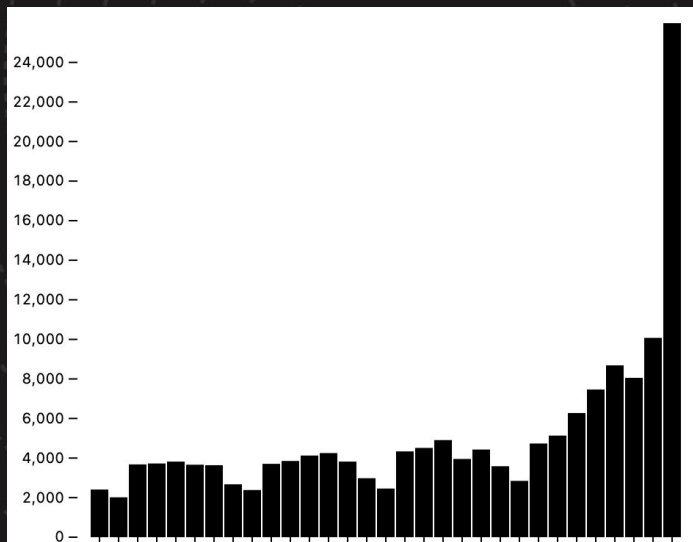


GREYNOISE
LABS

STORM ⚡ WATCH

Random Thoughts:

- New, and additional, war.
 - Cyberspace conflicts spill outside of warzones.
 - Triple check your perimeters.
- SMB scan traffic has 



S T O R M ⚡ W A T C H

Sift, continued...



Searching for gold
with your computer.

MakeAGIF.com

<https://sift.labs.greynoise.io>



GREYNOISE
LABS

S T O R M ⚡ W A T C H

DATELINE : 2023-10-10



GREYNOISE
LABS