**From:** IDFA-zTechnology <idfa-ztechnology-lists@lists.idfa.org> on behalf of Rob Carpenter <rcarpenter@idfa.org>
**Sent:** Wednesday, September 25, 2024 1:40 PM
**To:** Dairy Technology & Innovation Network (IDFA-zTechnology@lists.idfa.org)
**Subject:** IDFA's DTIN: Food and Ag-ISAC Weekly Report - Week Ending Sept 13, 2024
**Attachments:** ATT00001.txt

**Follow Up Flag:** Follow up
**Flag Status:** Completed

# Dairy Technology & Innovation Network

IDFA
International Dairy Foods Association

Dairy Technology & Innovation Network Members:

Below is this week's Weekly Report from the Food and Ag ISAC. As part of our ongoing partnership, the Food and Ag ISAC is allowing us to share this information which contains current news, intelligence, vulnerabilities & updates, and ransomware events.

Rob

**ROB CARPENTER**
Senior Director, Information Technology
International Dairy Foods Association

1250 H St. NW, Suite 900
Washington, DC 20005
**P:** 202.220.3501
www.idfa.org

Making a Difference for Dairy

Food Ag ISAC
An IT ISAC Community

WEEKLY REPORT

Celebrate Cybersecurity Awareness Month With Us!
Register today for our industry specific webinars.
SECURE OUR WORLD
IT ISAC
FOUNDED 2000

## CYBERSECURITY AWARENESS MONTH EVENTS

Throughout October, we will be celebrating and championing Cybersecurity Awareness Month with free webinars open to all in the industry. Check out each of the webinars below and register today!

- **October 9 at 2 PM ET** - Part I of Compliance Conundrums: The Intersection of Cybersecurity Reporting and Liability
- **October 29 at 4 PM ET** - CISO Confidential: AMA with CSaaS Security Leaders
- **October 30 at 2 PM ET** - Part II of Compliance Conundrums: The Intersection of Cybersecurity Reporting and Liability

REGISTER HERE

# Critical Vulnerabilities & Updates

## CISA Adds Several Known Exploited Vulnerabilities to Catalog

- CVE-2024-43461 Microsoft Windows MSHTML Platform Spoofing Vulnerability
- CVE-2024-6670 Progress WhatsUp Gold SQL Injection Vulnerability
- CVE-2014-0497 Adobe Flash Player Integer Underflow Vulnerability
- CVE-2013-0643 Adobe Flash Player Incorrect Default Permissions Vulnerability
- CVE-2013-0648 Adobe Flash Player Code Execution Vulnerability
- CVE-2014-0502 Adobe Flash Player Double Free Vulnerability
- CVE-2024-27348 Apache HugeGraph-Server Improper Access Control Vulnerability
- CVE-2020-0618 Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability
- CVE-2019-1069 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability
- CVE-2022-21445 Oracle JDeveloper Remote Code Execution Vulnerability
- CVE-2020-14644 Oracle WebLogic Server Remote Code Execution Vulnerability
- CVE-2024-8963 Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability

## Vulnerability Summary for the Week of September 9, 2024

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Notable Vulnerabilities:

- **Siemens--Industrial Edge Management Pro - CVE-2024-45032 - CVSS: 10**
  A vulnerability has been identified in Industrial Edge Management Pro (All versions < V1.9.5), Industrial Edge Management Virtual (All versions < V2.3.1-1). Affected components do not properly validate the device tokens. This could allow an unauthenticated remote attacker to impersonate other devices onboarded to the system.

- **GitLab--GitLab - CVE-2024-6678 - CVSS: 9.9**

An issue was discovered in GitLab CE/EE affecting all versions starting from 8.14 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2, which allows an attacker to trigger a pipeline as an arbitrary user under certain circumstances.

- **Docker -- desktop - CVE-2024-8696 - CVE-2024-8695 - CVSS: 9.8**
  A remote code execution (RCE) vulnerability via crafted extension publisher-url/additional-urls could be abused by a malicious extension in Docker Desktop before 4.34.2. A remote code execution (RCE) vulnerability via crafted extension description/changelog could be abused by a malicious extension in Docker Desktop before 4.34.2.

## CISA and FBI Release Secure by Design Alert on Eliminating Cross-Site Scripting Vulnerabilities

CISA and FBI released a Secure by Design Alert, Eliminating Cross-Site Scripting Vulnerabilities, as a part of our ongoing effort to reduce the prevalence of vulnerability classes at scale. Vulnerabilities like cross-site scripting (XSS) continue to appear in software, enabling threat actors to exploit them. However, cross-site scripting vulnerabilities are preventable and should not be present in software products.

CISA and FBI urge CEOs and other business leaders at technology manufacturers to direct their technical leaders/teams to review past instances of these defects and create a strategic plan to prevent them in the future.

## VMware Releases Security Advisory for VMware Cloud Foundation and vCenter Server

VMware released a security advisory addressing vulnerabilities in the VMware Cloud Foundation and the vCenter Server. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

CISA encourages users and administrators to review the following VMware security advisory and apply the necessary updates:

- VCDSA24968

## Ivanti Releases Admin Bypass Security Update for Cloud Services Appliance

Ivanti has released a security update to address an admin bypass vulnerability (CVE-2024-8963) affecting Ivanti Cloud Services Appliance (CSA) version 4.6.  A cyber threat actor could exploit this vulnerability in conjunction with CVE-2024-8190–detailed in a Sept. 13 Ivanti security advisory–to take control of an affected system. This vulnerability impacts all versions prior to patch 519. Ivanti has confirmed limited exploitation and recommends that users upgrade to CSA version 5.0, as version 4.6 is end-of-life and no longer supported. CISA urges users and administrators review the Ivanti security advisory and apply the necessary updates.

Note: CISA has added CVE-2024-8963 to its Known Exploited Vulnerabilities Catalog, which, per Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the specified due date to protect FCEB networks against active threats.

# ICS/OT Vulnerabilities

- ICSA-24-261-01 Siemens SIMATIC S7-200 SMART Devices
- ICSA-24-261-02 Millbeck Communications Proroute H685t-w
- ICSA-24-261-03 Yokogawa Dual-redundant Platform for Computer (PC2CKM)
- ICSA-24-263-01 Rockwell Automation RSLogix 5 and RSLogix 500
- ICSA-24-263-02 IDEC PLCs
- ICSA-24-263-03 IDEC CORPORATION WindLDR and WindO/I-NV4
- ICSA-24-263-04 MegaSys Computer Technologies Telenium Online Web Application
- ICSA-24-263-05 Kastle Systems Access Control System

# Open Source Intelligence

### Microsoft Confirms Second 0-Day Exploited by Void Banshee APT (CVE-2024-43461)

**SUMMARY**

CVE-2024-43461 is a critical spoofing vulnerability in Windows MSHTML, the engine responsible for rendering web content across various Microsoft applications such as Internet Explorer and Microsoft Office. This flaw was actively exploited by attackers in conjunction with CVE-2024-38112 as part of a sophisticated attack chain, prior to its discovery in July 2024. The attack was orchestrated by the Void Banshee APT group, known for targeting high-value entities across the globe. The campaign ultimately delivered the Atlantida malware, an info-stealer designed to exfiltrate sensitive data from compromised systems.

The attack chain began with the exploitation of CVE-2024-38112, which allowed a malicious URL file, masquerading as a seemingly harmless PDF, to bypass security measures and open in Internet Explorer instead of the more secure Microsoft Edge browser. Once the URL was accessed, it directed the victim to a malicious webpage controlled by the attackers. This webpage triggered the download of a specially crafted HTA file. The HTA file exploited CVE-2024-43461 to spoof its identity as a legitimate PDF file, thus disguising its malicious intent and tricking users into trusting and executing it.

Upon execution, the HTA file contained a malicious script that utilized PowerShell to further escalate the attack. The script downloaded and executed additional scripts, created new processes on the victim's machine, and initiated the download of trojan loaders. These loaders were specifically designed to deploy the Atlantida malware, a sophisticated info-stealer capable of collecting and transmitting sensitive information back to the attackers. The malware was particularly dangerous as it allowed the attackers to maintain a persistent foothold in the targeted system while exfiltrating valuable data.

**SOURCE**

- https://www.helpnetsecurity.com/2024/09/16/cve-2024-43461-exploited/
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43461

---

## Phishing Pages Delivered Through Refresh HTTP Response Header

### SUMMARY

Palo Alto Networks Unit 42 researchers are warning of ongoing large-scale phishing campaigns that abuse the refresh HTTP response header to direct end users to malicious domains designed to gather credentials. While the refresh header is not apart of the official HTTP standard, it is commonly supported by web browsers to either refresh or redirect a page when a specified amount of time has passed after the page is fully loaded. “Unlike other phishing webpage distribution behavior through HTML content, these attacks use the response header sent by a server, which occurs before the processing of the HTML content. Malicious links direct the browser to automatically refresh or reload a webpage immediately, without requiring user interaction. By carefully mimicking legitimate domains and redirecting victims to official sites, attackers can effectively mask their true objectives and increase the likelihood of successful credential theft,” noted researchers in a recent blog post.

### SOURCE

- https://unit42.paloaltonetworks.com/rare-phishing-page-delivery-header-refresh/

---

## D-Link Patches Critical Router Vulnerabilities

### SUMMARY

D-Link has fixed a couple of vulnerabilities impacting several of its wireless router models: COVR-X1870, DIR-X5460, and DIR-X4860. Three of the flaws have been rated critical in severity and are being tracked as CVE-2024-45694, CVE-2024-45695, CVE-2024-45697 respectively. CVE-2024-45694 and CVE-2024-45695 have been described as stack-based buffer overflow issues in the web service of several wireless routers and can be exploited by remote unauthenticated attackers to execute arbitrary code on the affected devices. CVE-2024-45697, on the other hand can allow actors to log in to vulnerable routers using hardcoded credentials. Two other flaws were fixed, which have been rated high in severity. The first one tracked as CVE-2024-45696, could allow attackers to enable the telnet service and use hardcoded credentials to log in to the device. The second flaw, tracked as CVE-2024-45698, relates to an improper input validation issue in the telnet service and can allow actors to login and execute OS commands with hard-coded credentials on vulnerable devices.

**SOURCE**

- https://www.securityweek.com/d-link-patches-critical-router-vulnerabilities/
- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412

# Monthly Ransomware Update

The companies listed below were listed on ransomware leak sites or reported to us via reliable third party sources. While the company was listed, we cannot confirm the legitimacy of an attack or it's impact to the listed organization. This information is being shared for your situational awareness, users should look for official announcements from potentially impacted victims.

### September 18, 2024 - Nat Co Global - Cactus

Natco Global is involved in the distribution and supply of agricultural products and services. A breach could impact the supply chain of essential agricultural inputs.

Cactus is a relatively new group which often avoids attention due to it’s much smaller set of victims. That being said, the group has made a name for itself by compromising several large commercial entities including some of the largest companies in the United States, Italy, the United Kingdom, Switzerland, and France. This group is known for breaking into networks by exploiting known vulnerabilities in VPN appliances and Qlik Sense software. They are also known to carry out phishing attacks, purchase stolen credentials through initial access brokers, and to partners with malware distributors.

### September 19, 2024 - Sunrise Farms - Fog

Non-GMO feeds and pasture- raised beef, pork, lamb, poultry, eggs, and raw honey.

Fog ransomware emerged on the landscape earlier this year.  The victims are typically located in the United States, and the group appears to prefer targets in the education and recreation sector.  Fog appears to be a Ransomware-as-a-service (RaaS) operation and works with multiple affiliates who actually carry out the attacks and execute the ransomware.  Researchers from Arctic

Wolf say “in each of the cases investigated, forensic evidence indicated that threat actors were able to access victim environments by leveraging compromised VPN credentials. Notably, the remote access occurred through two separate VPN gateway vendors.  Early in one of the cases, pass-the-hash activity was observed against administrator accounts which were subsequently used to establish RDP connections to Windows Servers running Hyper-V and Veeam. In another case, evidence of credential stuffing was observed, which was thought to facilitate lateral movement throughout the environment. In all cases, PsExec was deployed to several hosts, and RDP/SMB were used to access targeted hosts” (Arctic Wolf, 2024).  On Windows Servers that the threat actors interacted with, Windows Defender was disabled by the threat actors. Threat actors were observed encrypting VMDK files in VM storage and deleting backups from object storage in Veeam.  Notably, this group does not appear to have a data leak website, they are simply interacting with victims via Tor and will provide a decryptor upon ransom demands being met.

### September 19, 2024 - Satia Group - ValenciaLeaks

Likely involved in food distribution or agriculture-related services. A security incident could disrupt their operations and affect the delivery of food products.

ValenciaLeaks refers to a newly emerged ransomware group, known as Valencia Ransomware. This group has gained attention for its swift attacks on several major organizations, including the City of Pleasanton in California, Duopharma Biotech in Malaysia, Globe Pharmaceuticals in Bangladesh, Satia Industries in India, and the Spanish fashion retailer Tendam.

Valencia's tactics include stealing sensitive data and then leaking it on dark web platforms to extort their victims. For instance, they claimed to have stolen 304 GB of data from Pleasanton, which includes personal and financial details like credit card numbers and employee information. They have also leaked employee data and product details from other companies they've targeted. Although their operations are still new, experts consider their claims credible based on early analysis of the stolen data.

Interestingly, some experts have linked Valencia to a cybercriminal named LoadingQ, who has been active in underground hacking forums, suggesting that the group may be connected to other well-established cyber criminal activities.

### September 19, 2024 - Agri Cola - Qilin

This company is directly involved in agricultural production or services. A breach could compromise sensitive data regarding agricultural practices or disrupt their operations.

“Agenda ransomware was first observed in July of 2022. Agenda is written in Golang and also referred to as ‘Qilin’. Agenda ransomware supports multiple encryption modes; all of which are controlled by the operator. Agenda actors practice double extortion – demanding payment for a decryptor, as well as for the non-release of stolen data” (SentinelOne).

“Agenda ransomware targets its victims through phishing and spear phishing emails. They are also known to leverage exposed applications and interfaces such as Citrix and remote desktop protocol (RDP). Agenda ransomware has some customization options, which include changing the filename extensions of encrypted files and the list of processes and services to terminate. It supports several encryption modes that the ransomware operator can configure through the encryption setting. The ‘help’ screen displays the different encryption modes available: skip-step, percent, and fast” (SentinelOne).

### September 19, 2024 - Duo Pharma - ValenciaLeaks

Focused on biotechnological advancements, possibly including those that enhance food safety or agricultural productivity. A breach could affect the development or safety of agricultural biotech solutions.

ValenciaLeaks refers to a newly emerged ransomware group, known as Valencia Ransomware. This group has gained attention for its swift attacks on several major organizations, including the City of Pleasanton in California, Duopharma Biotech in Malaysia, Globe Pharmaceuticals in Bangladesh, Satia Industries in India, and the Spanish fashion retailer Tendam.

Valencia's tactics include stealing sensitive data and then leaking it on dark web platforms to extort their victims. For instance, they claimed to have stolen 304 GB of data from Pleasanton, which includes personal and financial details like credit card numbers and employee information. They have also leaked employee data and product details from other companies they've targeted. Although their operations are still new, experts consider their claims credible based on early analysis of the stolen data.

Interestingly, some experts have linked Valencia to a cybercriminal named LoadingQ, who has been active in underground hacking forums, suggesting that the group may be connected to other well-established cyber criminal activities.

### September 19, 2024 - Compass Group - Medusa

A major player in food services, Compass Group provides catering and food management solutions. A breach could impact food safety protocols and service delivery, affecting numerous clients across various sectors.

“Medusa Ransomware is a variant that was believed to have emerged in June 2021 and has been becoming increasingly prolific as of late. While “Medusa” has been a commonly used in the name of other ransomware, malware, and botnets, it is distinct from its similarly named competitors (such as MedusaLocker). The ransomware claims to exfiltrate data from compromised organizations to perform a “double-extortion attack”, this is a type of attack in which the threat actor will not only encrypt compromised systems, but also sell or release the exfiltrated data publicly if a ransom is not met. Medusa Ransomware uses a .MEDUSA file extension for files it encrypts. Medusa Ransomware is considered to be an active threat, and thus poses a significant and present risk that should be ascertained and prepared for” (CyborgSecurity, 2024).

### September 20, 2024 - Aroma TR - RansomHub

AROMA Bursa Meyve Suları ve Gıda Sanayi A.Ş. was established on 1968 in Gürsu district of Bursa. In the company which was established with multi partners, Duruk Group bought the majority share in 1991 and took over the management. With the investment move started in 1991, the amount of fruits processed was increased every day and increased from 20.000 tons to 125.000 tons per year, and Aroma became one of the leading fruit juice filling facilities.

We have noted several attacks against the food and agriculture sector by Ransomhub. The cybercriminal group Scattered Spider has allegedly started using Qilin and Ransomhub in recent attacks. “Ransomhub, a new ransomware group, has targeted the SCADA system of a Spanish bioenergy plant, Matadero de Gijón, which highlights the critical security risks associated with Industrial Control Systems (ICS) across various industries. Since 2022, numerous cyberattacks have exploited vulnerabilities in ICS, causing significant disruptions to operations and infrastructure." (CyberSecurityNews, 2024).

CISA recently released a STOPRansomware Report on the group, which can be found below: https://www.cisa.gov/news-events/alerts/2024/08/29/cisa-and-partners-release-advisory-ransomhub-ransomware

---

Visit Our Website

Food Ag ISAC

An IT ISAC Community

Our mailing address is:
Food and Ag-ISAC 9401 Centreville Rd Manassas, VA 20110 USA