# UNITE 2024

## CISA - Your Official Source of Cybersecurity Alerts and Vulnerability Management

**Session 6526, March 5th, 12:15PM ET**

**Guy Bonney**
**President**
**MGS, Inc.**

MGS INC
Computer Business Solutions

# MGS, Inc.

- Software Engineering, Product Development & Professional Services firm founded in 1986
- We solve business problems with:
  - Products:
    - SightLine™ Performance/Capacity - Engineering
    - MGSWEB Web Services
    - Deliver/Retrieve
    - C.A.T.T. / CATTSecured Terminal Emulator
    - File Manager for MCP
  - Professional Services
    - Performance/Capacity Management
    - Installation Services
    - MCP Training
  - Software Engineering Services
    - ClearPath MCP
    - Windows

MGS INC
Computer Business Solutions

# CISA is

- Cybersecurity and Infrastructure Security Agency (CISA) - America's Cyber Defense Agency.
- An Agency in the Department of Homeland Security
- Responsible for Cybersecurity direction to Federal Civilian Executive Branch (FCEB) agencies AND
- infrastructure, governments, businesses, schools, and all other organizations.

MGS INC
Computer Business Solutions

# With whom does CISA work

- US Agencies
  - National Security Agency
  - Federal Bureau of Investigation
  - Department of Energy
  - Environmental Protection Agency
  - Transportation Security Agency
- Foreign Agencies: UK National Cyber Security Centre, Australian Signals Directorate, Canadian Centre for Cyber Security, New Zealand National Cyber Security Centre

MGS INC
Computer Business Solutions

# What do they do?

- Publish and disseminate information:
  - Alerts and Advisories
  - Process and procedure guidance documentation
  - Recommend security frameworks
  - Information on Ransomware and defenses
  - Training in Cyber and Physical Security
  - Activities of State Actors
  - Guidance in seeking help
- Coordinate above activities with US Cyber agencies and Allied Cyber Agencies

MGS INC
Computer Business Solutions

# CISA Weekly Vulnerability Email

- Date: Mon, 04 Mar 2024 22:57:51 +0000
- To: Guy.Bonney@mgsinc.com
- Reply-To: CISA@messages.cisa.gov
- From: "CISA" CISA@messages.cisa.gov

- You are subscribed to Vulnerability Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

- Vulnerability Summary for the Week of February 26, 2024
- 03/04/2024 04:03 PM EST

MGS INC
Computer Business Solutions

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. NVD is sponsored by CISA. 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.

Vulnerabilities are based on the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

High: vulnerabilities with a CVSS base score of 7.0–10.0
Medium: vulnerabilities with a CVSS base score of 4.0–6.9
Low: vulnerabilities with a CVSS base score of 0.0–3.9

# CISA Weekly Vulnerability Email Alert

- google -- chrome
- Type Confusion in V8 in Google Chrome prior to 122.0.6261.94 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) 2024-02-29 not yet calculated CVE-2024-1938
- https://nvd.nist.gov/vuln/detail/CVE-2024-1938
- Chrome-cve-admin@google.com

MGS INC
Computer Business Solutions

# CISA VMware Alert Example

- vmware -- aria_automation/cloud_foundation
- Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. 2024-01-16 9.9 CVE-2023-34063

- https://nvd.nist.gov/vuln/detail/CVE-2023-34063
- security@vmware.com

MGS INC
Computer Business Solutions

# CISA VMware Alert Today

- You are subscribed to Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.
- VMware Releases Security Advisory for Multiple Products
- 03/06/2024 07:00 AM EST
- VMware released a security advisory to address multiple vulnerabilities in ESXi, Workstation, Fusion, and Cloud Foundation. 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:
- https://www.vmware.com/security/advisories/VMSA-2024-0006.html

MGS INC
Computer Business Solutions

# CISA & Partners Release Advisory on Threat Actors

- Today, CISA and the following partners released joint Cybersecurity Advisory
  - Federal Bureau of Investigation (FBI)
  - Multi-State Information Sharing & Analysis Center (MS-ISAC)
  - Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
  - United Kingdom National Cyber Security Centre (NCSC-UK)
  - Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment
  - New Zealand National Cyber Security Centre (NCSC-NZ)
  - CERT-New Zealand (CERT NZ)
- Issues with Ivanti Connect Secure and Policy Secure tools
- CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893
- The Ivanti Integrity Checker Tool is not sufficient to detect compromise

MGS INC
Computer Business Solutions

# CISA Emergency Directive Example

- ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities
- January 19, 2024
- Related topics: Cybersecurity Best Practices
- Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v). These directives do not apply to statutorily defined “national security systems” nor to systems operated by the Department of Defense or the Intelligence Community.
- https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

MGS INC
Computer Business Solutions

# Cyber Education & Training Updates - March - April 2024

- CISA has recently announced two new collaborative efforts:
- The CyberSkills2Work program, part of the University of West Florida Center for Cybersecurity, is an intensive online cybersecurity training program focused on critical infrastructure security and industrial control systems security. It is designed to help individuals launch or advance cybersecurity careers, with an emphasis on federal, state, and local government personnel, transitioning military, veterans, women, and underrepresented minorities.
- https://cyberskills2work.org/i/
- CISA offers new micro-challenges on Try Cyber For K-12 students and individuals looking to reskill or transition from a non-cyber career
- https://trycyber.us/

MGS INC
Computer Business Solutions

# CISA Cybersecurity Advisories

- CISA, FBI, and HHS Release an Update to #StopRansomware Advisory on ALPHV Blackcat
- 02/27/2024 04:45 PM EST
- Provides new indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the ALPHV Blackcat ransomware as a service (RaaS). ALPHV Blackcat affiliates have been observed primarily targeting the healthcare sector.
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
- For more on ransomware, visit stopransomware.gov.
- Report ransomware to FBI at CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

MGS INC
Computer Business Solutions

# CISA Advisory on State Actors

- CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors
- CISA, in partnership with UK National Cyber Security Centre (NCSC) and other U.S. and international partners released the joint advisory, SVR Cyber Actors Adapt Tactics for Initial Cloud Access. This advisory provides recent tactics, techniques, and procedures (TTPs) used by Russian Foreign Intelligence Service (SVR) cyber actors—also known as APT29, the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard—to gain initial access into a cloud environment.
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

MGS INC
Computer Business Solutions

# CISA Known Exploited Vulnerabilities Catalog

- CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.
- 03/04/2024 12:00 PM EST
- CVE-2024-21338 Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability.
- https://nvd.nist.gov/vuln/detail/CVE-2024-21338

MGS INC
Computer Business Solutions

# CISA Industrial Control Systems Advisories

- CISA Releases Two Industrial Control Systems Advisories
- 02/27/2024 07:00 AM EST

- CISA released two Industrial Control Systems (ICS) advisories on February 27, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- ICSA-24-058-01 Mitsubishi Electric Multiple Factory Automation Products
- ICSMA-24-058-01 Santesoft Sante DICOM Viewer Pro

MGS INC
Computer Business Solutions

# CISA Resource Guides

- CISA Releases Resource Guide for University Cybersecurity Clinics
  02/28/2024 02:00 PM EST
- This Guide outlines ways CISA can partner with and support cybersecurity clinics and their clients.
- University cybersecurity clinics train students from diverse backgrounds and academic expertise to strengthen the digital defenses of non-profits, hospitals, municipalities, small businesses, and other under-resourced organizations.
- https://www.cisa.gov/resources-tools/resources/resources-cybersecurity-clinics

MGS INC
Computer Business Solutions

# Questions?

- Thank you for your attention
- Are there any questions?

This presentation is available at:
www.mgsinc.com/download.html

MGS INC
Computer Business Solutions

# Contact Information

- Guy Bonney
  - President
  - Guy.Bonney@mgsinc.com
  - MGS, Inc.

    11506 Allecingie Pkwy, Suite 2B
    Richmond, VA 23235
  - Phone: 804-379-0230
    Fax: 804-379-1299

    Mobile: 703-395-6626
  - www.mgsinc.com

MGS INC
Computer Business Solutions