VULCAN.

VOYAGER18

Q1 2023
Vulnerability Watch

Quarterly trends, themes and insights from the world of cyber security vulnerabilties

Table of contents

Introduction

This report identifies some of the most noteworthy vulnerabilities from the first quarter of 2023. Throughout the report — updated as of March 26th 2023 — we highlight the potential impact of these vulnerabilities, and offer practical insights for organizations to bolster their vulnerability risk management efforts. We also provide comprehensive technical details about CVEs, going beyond just their severity rating in the Common Vulnerability Scoring System (CVSS). We also cover their Exploitability Score (EPSS) and presence in the catalog maintained by the Cybersecurity and Infrastructure Security Agency (CISA), among other information.

The story of Q1 2023

The Coalition Cyber Threat Index 2023[1] predicts more than 1,900 new CVEs per month in 2023, including 270 high risk vulnerabilities. Whether this large volume of fresh vulnerabilities is due to improvements in detection, or a drop in overall code quality, is difficult to tell without specific research.

Overall, while there were several significant vulnerabilities in Q1, we identified **systems management software as a particular area of interest to attackers**, with some widely-used products heavily impacted.

IT management software under attack

Vulnerabilities in IT management tools and services appear to be a common theme in Q1 2023, as shown by many of the examples below. It is crucial for IT managers to include cyber security as a crucial aspect of their management practices, and to work with their teams and other stakeholders to manage risk. This is especially important given the trend towards attacks against IT management vulnerabilities in 2023's first quarter.

IT management refers to the tools, procedures, and guidelines used to supervise and maintain an organization's information technology infrastructure. This infrastructure often includes hardware, software, networks, and the data that resides within. This team is often responsible for an organization's cloud infrastructure as well. Poor system configurations, a lack of patching and updates, lax password policies, and insufficient employee training are all examples of poor IT management practices that can lead to exploitable vulnerabilities. Which tools IT management deploys, and how they allocate their resources, can have a huge impact on the organization's risk posture.

[1] Cyber Threat index 2023 | Coalition Inc

Notable vulnerabilities of Q1 2023

CVE-2022-3875

Affected products:	Click Studios Passwordstate and Passwordstate Browser Extension in Google Chrome
Product category:	IT management (Password manager)
Severity:	CVSS: 7.5 | EPSS: 0.18%
Type:	Authentication bypass
Impact:	Arbitrary code execution or actions performed with elevated privileges
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2022-3875, a critical vulnerability in Passwordstate and its Chrome extension, allows attackers to bypass authentication and access plaintext passwords. The issue was resolved in build 9611 on Sep 5, 2022. Users should urgently upgrade to eliminate the vulnerability. Although active exploitation is unconfirmed, proof-of-concept code is available.

CVE-2023-20025

Affected products:	Cisco Small Business RV042 Series Routers
Product category:	Network devices
Severity:	CVSS: 9.8 | EPSS: 0.19%
Type:	Authentication bypass
Impact:	Incorrect user input validation of incoming HTTP packets
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-20025 affects Cisco Small Business RV042 Series Routers, enabling unauthenticated remote attackers to bypass authentication. This critical vulnerability won't be fixed as the routers are end-of-life. Owners should remove end-of-life routers from service. If replacement is not possible, they should reduce the risks by disabling remote management and limiting access to the management console as much as practical.

CVE-2022-3656

Affected products:	Google Chrome and Chromium
Product category:	Browser vulnerability
Severity:	CVSS: 8.8 | EPSS: 0.13%
Type:	Insufficient data validation
Impact:	Bypassed file system restrictions via a crafted HTML page
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

A vulnerability in Google Chrome before version 107.0.5304.62, CVE-2022-3656 lets a remote attacker use a specially crafted HTML page to bypass file system restrictions. The Imperva Red Team discovered this vulnerability, which has been assigned a medium severity. This vulnerability impacts over 2.5 billion users of Chrome and Chromium-based browsers, which hold a combined market share of more than 70%. Google resolved the vulnerability by releasing version 107.0.5304.62.

CVE-2021-35394

Affected products:	UDPServer in Realtek Jungle SDK
Product category:	IOT vulnerability
Severity:	CVSS: 9.8 | EPSS: 96.82%
Type:	Remote code execution
Impact:	Command injection
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2021-35394, a critical vulnerability in Realtek Jungle SDK v2.x to 3.4.14B, results from multiple memory corruption issues and an arbitrary command injection vulnerability. It has been widely exploited, including by the 'RedGoBot' botnet malware targeting IoT devices. Despite Realtek's patch release, vendors' delayed responses have hindered user protection. Users should ensure their devices have the latest updates to avoid vulnerability exploitation.

CVE-2022-31704

Affected products:	VMware vRealize Log Insight
Product category:	IT management (Log management)
Severity:	CVSS: 9.8 | EPSS: 0.25%
Type:	Broken access control
Impact:	Code injection into files of impacted appliance
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2022-31704, found in VMware vRealize Log Insight, is a critical vulnerability that allows for remote code execution. This vulnerability has a CVSS base score of 9.8 and can be exploited as part of low-complexity attacks that don't require user interaction. VMware released security updates to address these vulnerabilities on January 25, 2023, and it is recommended that users upgrade to version 8.10.2 to prevent potential exploitation.

CVE-2022-31706

Affected products:	VMware vRealize Log Insight
Product category:	IT management (Log management)
Severity:	CVSS: 9.8 | EPSS: 0.25%
Type:	Directory traversal
Impact:	Code injection into files of impacted appliance
PoC:	No
Exploit in the wild:	Yes
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

Another critical vulnerability affecting VMware vRealize Log Insight, CVE-2022-31706 also has a CVSS base score of 9.8, and carries a similar impact when exploited, this time as a directory traversal vulnerability. It is again recommended that users upgrade to version 8.10.2 to prevent exploitation.

CVE-2022-47966

Affected products:	Multiple ManageEngine products, including ServiceDesk Plus, Password Manager Pro, and others
Product category:	IT management (Password manager)
Severity:	CVSS: 9.8 | EPSS: 97.38%
Type:	Remote code execution
Impact:	Arbitrary code execution
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

ManageEngine

CVE-2022-47966, a pre-authentication remote code execution vulnerability, affects 24 ManageEngine on-premise products due to Apache xmlsec 1.4.1 usage. Products like ServiceDesk Plus through 14003 are at risk. The vulnerability has been exploited in the wild, with a PoC available. It's awaiting reanalysis, but users should apply patches or workarounds immediately to reduce risk.

CVE-2021-21974

Affected products:	VMware ESXi
Product category:	IT management
Severity:	CVSS: 8.8 | EPSS: 95.26%
Type:	Heap overflow
Impact:	Remotely executed malicious code on affected systems
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

vmware

CVE-2021-21974 is a heap overflow vulnerability in OpenSLP used in ESXi. It can be exploited by malicious actors in the same network segment. VMware released patches in 2019, however many ESXi servers remain unpatched and vulnerable, with ransomware campaigns exploiting it. Organizations should patch vulnerable ESXi servers, or deploy compensating controls where patches can't be deployed.

CVE-2022-39952

Affected products:	FortiNAC
Product category:	IT management (Network access)
Severity:	CVSS: 9.8 | EPSS: 96.71%
Type:	External control
Impact:	Executed arbitrary writes on vulnerable systems
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

Two critical vulnerabilities affect Fortinet's FortiNAC secure access control solution, CVE-2022-39952 and CVE-2021-42756 (below). In the case of CVE-2022-39952, the vulnerability allows unauthenticated attackers to perform arbitrary writes. A PoC exploit has been released. Fortinet resolved the issue in specific FortiNAC versions; and admins should update promptly.

CVE-2021-42756

Affected products:	FortiWeb
Product category:	IT management
Severity:	CVSS: 9.8 | EPSS: 0.39%
Type:	Stack-based buffer overflow
Impact:	Remotely executed arbitrary code
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

Fortinet's proxy daemon in FortiWeb is affected by a severe vulnerability identified as CVE-2021-42756. The vulnerability has been publicly disclosed and assigned a "very critical" severity rating. It is a stack-based buffer overflow vulnerability [CWE-121] that may enable an unauthenticated remote attacker to execute arbitrary code on the vulnerable system. Fortinet has addressed this vulnerability by releasing security advisories and patches.

CVE-2023-22501

Affected products:	Jira Service Management Server and Data Center
Product category:	Third party software
Severity:	CVSS: 9.1 | EPSS: 0.51%
Type:	Authentication bypass
Impact:	Attacker can impersonate user and gain access
PoC:	No
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-22501 affects Jira Service Management Server and Data Center offerings. Under certain conditions, the vulnerability allows an attacker to impersonate another user and gain access to a Jira Service Management instance. Atlassian has issued a vulnerability advisory, urging users to patch their systems as soon as possible. Unfortunately, determining whether a Jira Service Management instance has been compromised is not possible. Users can, however, view a list of potentially affected accounts after upgrading or updating the instance with the version-specific JAR file.

CVE-2023-21716

Affected products:	Microsoft 365 applications, MS office, MS word, MS SharePoint
Product category:	Third party software
Severity:	CVSS: 9.8 | EPSS: 17.94%
Type:	Remote code execution
Impact:	Escalated code embedded in an RTF file
PoC:	Yes
Exploit in the wild:	No
CISA catalog:	No
Remediation action:	Read more
MITRE advisory:	Read more

In February 2023, a heap corruption vulnerability was detected in Microsoft Word's RTF Parser, and documented in CVE-2023-21716. Attackers can use a maliciously crafted file to exploit a remote code execution vulnerability. The remote code will run with the victim's privileges. This vulnerability has received a CVSS Version 3.x severity score of 9.8.

CVE-2023-23397

Affected products:	Microsoft Outlook
Product category:	Third party software
Severity:	CVSS: 9.8 | EPSS: 47.53%
Type:	Elevation of Privilege (EoP)
Impact:	Privilege escalation vulnerability, Authentication bypass
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

CVE-2023-23397 is a critical privilege elevation vulnerability in Microsoft Outlook for Windows. It was assigned a CVSSv3 score of 9.8 and was exploited in the wild. The vulnerability can be exploited by sending a malicious email to an Outlook version that is vulnerable. It is strongly advised that the vulnerability be patched as soon as possible.

CVE-2022-35914

Affected products:	Htmlawed, a third-party library in Teclib GLPI
Product category:	IT management
Severity:	CVSS: 9.8 | EPSS: 96.67%
Type:	Remote code execution
Impact:	Arbitrary code execution
PoC:	Yes
Exploit in the wild:	Yes
CISA catalog:	Yes
Remediation action:	Read more
MITRE advisory:	Read more

GLPI through version 10.0.2 is affected by CVE-2022-35914, a critical PHP code injection vulnerability with a 9.8 CVSS score. It's been exploited extensively, impacting poorly maintained servers. Different from CVE-2022-31061, the issue is resolved in GLPI 10.0.3 or later. Organizations should upgrade, and CISA's Known Exploited Vulnerabilities Catalog offers additional guidance.

Summary

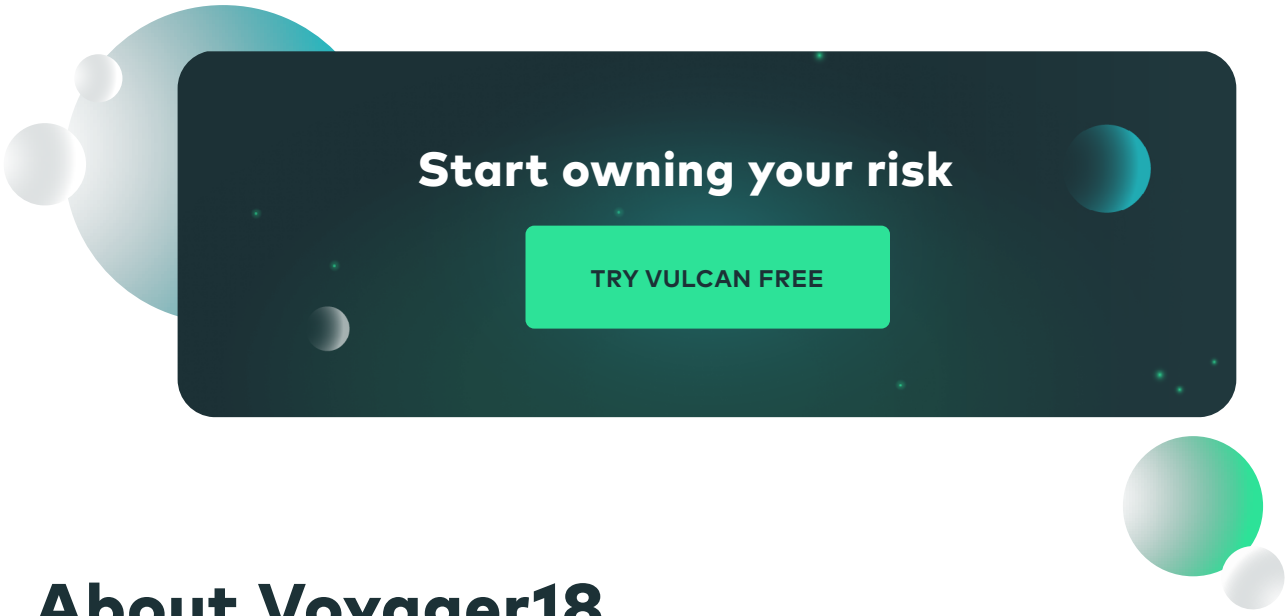
As cyber criminals continue to evolve their tactics and become more sophisticated, leveraging automation, cloud environments, third-party software, and IoT devices, it is imperative that organizations remain vigilant and adaptive in their cyber security posture.

IT management services, in particular, need to prioritize cyber security as an essential aspect of their practices. By staying informed about the latest threats and vulnerabilities, organizations can better protect their valuable assets and minimize the risk of successful attacks. This report has provided practical insights and actionable recommendations to help organizations bolster their defenses against the ever-changing cyber threat landscape.

As we move forward, it is crucial for organizations to stay updated on emerging cyber security trends, adopt a proactive approach to vulnerability management, and invest in continuous training and education for their IT teams. By doing so, they can effectively mitigate the potential impact of these vulnerabilities and maintain a strong security posture in the face of ongoing cyber challenges.

About Vulcan Cyber

Vulcan Cyber enables security teams to effectively manage and reduce vulnerability risk across IT and cloud-native surfaces. The platform consolidates vulnerability scan and threat intelligence data from all attack surfaces and provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a 2019 Gartner Cool Vendor and as a 2020 RSA Conference Innovation Sandbox finalist. Prominent security teams, such as those at Mandiant, Deloitte, and Snowflake, trust Vulcan Cyber to help them own their risk.



About Voyager18

The Vulcan Cyber research team, also known as Voyager18, is a team of cyber experts working to leverage machine learning and cyber research to ensure Vulcan Cyber remains a cyber security leader. The team's main objective is to research the latest cyber risk trends, including new attack types and remediations. The team is also responsible for bringing innovation to the Vulcan Cyber platform so that our customers get improved and customized cyber risk management capabilities. This includes research of more specific and accurate risk calculations, and the launch of VulnRX — a dynamic library of vulnerabilities and their remediation actions. Recently, the team mapped out the MITRE ATT&CK framework to relevant CVEs, providing granular insights into the most critical vulnerabilities. The full research is available here.

Stay up to date with the latest research here >>