Threat Intel Report

Prepared by:

Converge Cybersecurity Practice

November 29, 2022

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

convergetp.com | 800.747.8585

It's the fourth quarter of the year and time to fulfill outstanding compliance requirements. And while we're no fan of so-called "check-box compliance," external pressure to increase the organization's security posture has its place. Like a twice-yearly dental checkup, meeting yearly compliance obligations can help identify possible cracks in our critical infrastructure and polish up our readiness.

It's important to remember, however, that compliance alone is not enough. The fact that employees may be squeezing in their annual security awareness training videos is a good thing, but it doesn't mean they won't fall victim to a phishing attack. Your annual penetration test will pinpoint valid issues, but if your digital footprint constantly changes, those results will be obsolete within Q1.

Cybersecurity is a continuous process of assessing risks, enforcing and adapting controls, and testing those controls. Building a culture of security from within will help ensure that compliance keeps its proper place—as a top priority, but not the ONLY security priority. The real priority is a cyber-resilient organization, day after day.

Situational Awareness

Dropbox developers hit by phishing attack

Dropbox announced in early November that a successful phishing attack against its employees resulted in a threat actor stealing code from 130 of its GitHub repositories. The attack targeted multiple employees and used emails impersonating the CircleCI DevOps integration platform to redirect users to a phishing landing page where they were asked to enter their GitHub credentials and one-time password.

Exposed in the repositories were Dropbox's modified copies of third-party libraries, internal prototypes, and tools and configuration files. The code and other data included names and email addresses belonging to Dropbox employees, customers, sales leads, and vendors. Dropbox emphasized that customer accounts and payment information were not impacted and that the repositories did not include code for their core apps or infrastructure.

In targeting developers, the attack underscored that highly technical users are not immune to phishing. Even the most skeptical, vigilant professional can fall prey to a carefully crafted message delivered in the right way at the right time, said Dropbox. To prevent such attacks in the future, the company is continuing its rollout of the WebAuthn form of multifactor authentication.

Hacked documents reveal Iran's digital surveillance capabilities

In late October, hacked internal documents from an Iranian cellular carrier revealed details of the Iranian government's digital surveillance and control capabilities. The government maintains tight control over the country's internet access, especially during periods of protest, and the documents explain how a system called SIAM may help achieve this.

SIAM is a web program used by Iran's Communications Regulatory Authority that integrates with Iranian cellular networks and enables its operators to monitor and control how individuals use their phones. The system allows for slowing data connections, breaking encryption, tracking phone users' movements, and can be queried for information about individual users such as personal details, location, and call contacts.

In the hands of a repressive regime that may be using it to track down protestors, SIAM represents the kind of big brother situation that digital privacy advocates have been concerned about for years.

Currently Active Threats

Exploitation

Converge Cybersecurity Threat Intelligence Group is tracking multiple exploits that are actively being utilized in attacks. We track not only what we encounter in client environments but also attacks seen around the world. The following vulnerabilities have been linked to ransomware and dropper incidents reported around the world this month.

CVE-2021-39144 (CVSS score: 8.5)

Products Affected: VMware Cloud Foundation with XStream versions before 1.4.19

Status: Update released

In July 2021, tens of thousands of publicly exposed hosts were reportedly affected by this vulnerability. According to search engine Shodan, Great Britain alone hosts 751 exposed instances. In November, our threat intelligence sources revealed 37 instances of outdated VMware software being actively exploited, 26 of which were in the US.

CVE-2020-3433 (CVSS score: 7.8)

Products Affected: Cisco AnyConnect Secure Mobility Client for Windows versions before 4.9.00086

Status: Update released

Last month, Cisco warned about additional attempted exploitation of this 2020 vulnerability. In our November threat intelligence sources, Converge Cybersecurity has identified 11 sightings related to this vulnerability exploited by active ransomware groups.

Threat actors

LockBit 3.0

Primary impact: Professional services, internet services, manufacturing

LockBit, one of the most destructive ransomware threats, claims French aerospace and defense group Thales and German multinational automotive group Continental among its most recent victims. LockBit appears to have made troves of stolen data from both organizations available on its leak site. Authorities in Canada recently arrested an alleged LockBit member for his participation in the group.

OPERA1ER

Primary impact: Banks, financial services, and telecoms organizations

Converge Cybersecurity recently began tracking a new Cobalt Strike command and control server within the United States, a geolocation that makes it easier to bypass detection mechanisms. We have associated this server with the threat actor known as OPERA1ER.

OPERA1ER has been linked to over 30 cyber attacks in Africa, Asia, and Latin America between 2018 and 2022. The attacks have led to thefts totaling at least $11 million, with actual damages estimated to be as high as $30

million. The group obtains initial access via phishing emails with hooks, such as postal delivery notifications and invoices.

Malware

Emotet

Primary impact: All organizations

After months of inactivity, Emotet is once again blasting out malicious emails to the tune of hundreds of thousands per day, according to Proofpoint. A Proofpoint researcher said that Emotet's new campaign uses stolen email reply chains to distribute malicious Excel attachments. The campaign also introduces a new Excel attachment template containing instructions for bypassing Microsoft's Protected View. The Emotet malware is downloaded as a DLL into multiple randomly named folders under *%UserProfile%\AppData\Local*. After being downloaded, it runs in the background and connects to its C2 server to receive instructions.

IOCs (SHA 256):

- ef2ce641a4e9f270eea626e8e4800b0b97b4a436c40e7af30aeb6f02566b809c
- aef461e917273a9e8eb9c26a670689b9e6d26d3efe363c0f44d3bab34a6d371b
- 6e8ccade5bca2836792a9e8e0b0d9e70070005af95a332380c76645287039fae
- 65f6bf1299c82659d54482d0d08ed38dcdf61826f7df7fb68301620933e61e16
- cd99b899c5a3d6ddb22969605b079375da897362b4d599fc9eebb1e21115a31d
- f9a9b01d460cf2e4ff970a3d7e9b0f7c4be4d5d209aac07d186eb75a84bafb0b

SocGholish

Primary impact: Organizations with extensive marketing campaigns or strong search engine optimization

Threat actors compromised the infrastructure of an undisclosed media company to inject malware known as SocGholish into a JavaScript file accessed by over 250 US news sites in a supply chain attack. Impacted geographic areas included Boston, New York, Chicago, Miami, Washington DC, Cincinnati, Palm Beach, and more. Proofpoint researchers, who are tracking the threat actor as TA569, say the threat actor's intended target is not the media industry but rather the consumers who visit the impacted sites.

Vulnerabilities

Converge Cybersecurity has identified the following recently disclosed vulnerabilities as potentially having the most impact on organizations.

OpenLiteSpeed Web Server

Multiple high-severity vulnerabilities were disclosed in the OpenLiteSpeed Web Server that, when chained together, could enable a threat actor to exploit the web server and achieve fully privileged remote code execution. OpenLiteSpeed (open source) versions 1.5.11 to 1.7.16 and LiteSpeed (enterprise) versions 5.4.6 to 6.0.11 are impacted by the issues. These vulnerabilities have been addressed in versions 1.7.17.1 and 6.0.12.

CVE-2022-0072 (CVSS Score: 5.8)
Directory traversal vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server dashboard allows path traversal.

CVE-2022-0073 (CVSS Score: 8.8)
Improper input validation vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server dashboard allows command injection.

CVE-2022-0074 (CVSS Score: 8.8)
Untrusted Search Path vulnerability in LiteSpeed Technologies OpenLiteSpeed Web Server container allows privilege escalation.

Citrix Gateway and Citrix ADC

Citrix urges customers to install security updates for newly discovered vulnerabilities in Citrix ADC and Citrix Gateway. Three vulnerabilities enable attackers to gain unauthorized access to the device, perform remote desktop takeover, or bypass the login brute force protection. No action is needed by customers of the cloud-based management services.

CVE-2022-27510 (CVSS Score: 9.8)
Critical-severity authentication bypassing using an alternate path or channel, exploitable only if the appliance is configured as a VPN (Gateway).

CVE-2022-27513 (CVSS Score: 9.6)
Insufficient verification of data authenticity, allowing remote desktop takeover via phishing. The flaw is exploitable only if the appliance is configured as a VPN (Gateway), and the RDP proxy functionality is configured.

CVE-2022-27516 (CVSS Score: 9.8)
Mechanism failure of login brute force protection. This vulnerability can only be exploited if the appliance is configured as a VPN (Gateway) or AAA virtual server with “Max Login Attempts” configuration.

RCE vulnerabilities in iOS and macOS

Apple released out-of-band patches for iOS and macOS to fix arbitrary code execution vulnerabilities in libxml2 library. Apple has made no statement on any of the vulnerabilities being exploited in the wild; however, a proof of concept with full technical details was published to GitHub.

CVE-2022-40303 (CVSS Score: 8.3)
An integer overflow was addressed through improved input validation. A remote user may be able to cause unexpected app termination or arbitrary code execution.

CVE-2022-40304 (CVSS Score: 8.2)
When an entity reference cycle is detected, the entity content is cleared by setting its first byte to zero. But the entity content might be allocated from a dict. In this case, the dict entry becomes corrupted, leading to logic errors, including memory errors such as double-frees.

Fortinet High-Severity Vulnerabilities

Six high-severity flaws were identified when Fortinet informed customers of 16 new vulnerabilities discovered within its products. The vulnerabilities impact FortiADC, FortiDeceptor, FortiManager, FortiTester, FortiSIEM, and FortiAnalyzer. The vulnerabilities can be exploited for privilege escalation, cross-site scripting attacks, obtaining sensitive information, denial-of-service (DOS) attacks, bypassing protections, executing arbitrary commands, and modifying settings.

CVE-2022-38374 (CVSS Score: 8.0)
An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiADC may allow a remote, unauthenticated attacker to perform a stored cross-site scripting attack via HTTP fields observed in the traffic and event log views.

CVE-2022-35851 (CVSS Score: 7.5)
An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiADC management interface may allow a remote and authenticated attacker to trigger a stored cross-site scripting attack via configuring a specially crafted IP address.

CVE-2022-38373 (CVSS Score: 7.3)
An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiDeceptor management interface may allow an authenticated user to perform a cross-site scripting attack via sending requests with specially crafted lure resource ID.

CVE-2022-39950 (CVSS Score: 7.6)
An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiManager and FortiAnalyzer report templates may allow a low-privilege-level attacker to perform a cross-site scripting attack by posting a crafted CKeditor "protected" comment as described in CVE-2020-9281.

CVE-2022-33870 (CVSS Score: 7.4)
An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.

CVE-2022-26119 (CVSS Score: 7.4)
An improper authentication vulnerability [CWE-287] in FortiSIEM may allow a local attacker with CLI access to perform operations on the GlassFish server directly via a hardcoded password.