CONAPO

SINDACATO AUTONOMO VIGILI DEL FUOCO

"nella nostra autonomia la Vostra sicurezza"

OBIETTIVO CO.NA.PO. 50 % + 1

Segreteria Generale
Vico del Fiore, 21/23 - 54011 - Aulla (MS)
Tel. 0187-421814
e-mail: nazionale@conapo.it
sito internet www.conapo.it

Roma, 4 Febbraio 2022

Prot. 019/22

Al Capo Dipartimento dei Vigili del Fuoco,
del Soccorso Pubblico e della Difesa Civile
Prefetto Laura LEGA

Al Capo del Corpo Nazionale dei Vigili del Fuoco
Ing. Guido PARISI

Al Direttore Centrale per le Risorse Umane
Dipartimento dei Vigili del Fuoco, Socc. Pubblico e Dif. Civile
Prefetto Fabio MARSILIO

Al Direttore Centrale per l'Emergenza il Socc. Tecnico e l'Ant. Boschivo
Dipartimento dei Vigili del Fuoco, Soccorso Pubblico e Difesa Civile
Ing. Marco GHIMENTI

Al Direttore Centrale per le Risorse Logistiche e Strumentali
Dipartimento dei Vigili del Fuoco, Soccorso Pubblico e Difesa Civile
Ing. Giovanni NANNI

Al Direttore Centrale per la Formazione
Dipartimento dei Vigili del Fuoco, Soccorso Pubblico e Difesa Civile
Ing. Gaetano VALLEFUOCO

e, p. c. **Al Sottosegretario di Stato per l'Interno**
On. Carlo SIBILIA

All'Ufficio III – Relazioni Sindacali
Dipartimento dei Vigili del Fuoco, Socc. Pubblico e Dif. Civile
Dott. Bruno STRATI

Oggetto: **Formazione Personale Ruolo Tecnico Informatico del CNVVF - sollecito.**

Solo poche settimane fa, questa O.S. CO.NA.PO. (ns prot. n. 08/22 del 09.01.2022, allegato 1) lamentava la scarsa attenzione riguardo la formazione del personale del Ruolo Tecnico Informatico evidenziando inoltre la urgente necessità di offrire agli informatici del Corpo nazionale tutti gli strumenti e le conoscenze (supportate da idonee certificazioni) necessari per operare ed interfacciarsi anche con enti ed aziende esterni, **tra cui corsi di "Cybersecurity".**

In data 27 gennaio u.s., la Direzione Centrale per le Risorse Logistiche e Strumentali inviava informative (prot. nn. 2291 e 2292, allegati 2 e 3) alle strutture centrali e periferiche del C.N.VV.F. nelle quali **si chiede esplicitamente al personale informatico di effettuare attività specialistica di "Cybersecurity"** al fine di scongiurare la presenza nei nostri sistemi informatici, di vulnerabilità causate da software malevoli. **Il tutto nella completa assenza di procedure e/o istruzioni tecniche da seguire** per garantire in concreto l'efficace messa in sicurezza dei Sistemi informativi del Dipartimento VV.F. ed il monitoraggio da parte delle Strutture Centrali del Corpo.

Circolari che ci sembrano assomigliare più a dei "manleva di responsabilità per i Dirigenti" piuttosto che attività volte alla concreta, tempestiva ed efficace soluzione dei problemi di tipo informatico.

Se da un lato non possiamo che compiacerci di essere stati lungimiranti come O.S. nel rappresentare le criticità del settore e nell'aver addirittura chiesto una formazione specifica in materia di "**Cybersecurity**", dall'altro lato non possiamo non rammaricarci nel vedere che codesto Dipartimento VV.F. continua a perseverare secondo una prassi assurdamente lontana dalle reali necessità del mondo I.C.T. (Information Communication Technology) e tristemente rivolta per lo più a risolvere i problemi del Corpo nazionale in materia "sfruttando" la buona volontà del personale informatico che in autonomia ed a proprie spese investe nella propria formazione.

Premesso ciò, **questa O.S. CO.NA.PO. ribadisce la necessità di istituire tempestivamente un tavolo tecnico per l'aggiornamento ed il potenziamento formativo del personale tecnico-informatico.**

In attesa di cortese riscontro, si porgono distinti saluti.

IL SEGRETARIO GENERALE AGGIUNTO
CONAPO Sindacato Autonomo VVF
Marco Piergallini

Allegati come al testo

CONAPO SINDACATO AUTONOMO VIGILI DEL FUOCO
"nella nostra autonomia la Vostra sicurezza"
OBIETTIVO CO.NA.PO. 50 % + 1

Segreteria Generale
Vico del Fiore, 21/23 - 54011 - Aulla (MS)
Tel. 0187-421814
e-mail: nazionale@conapo.it
sito internet www.conapo.it

Roma, 9 Gennaio 2022

Prot.08/22

Al Capo Dipartimento dei Vigili del Fuoco
del Soccorso Pubblico e della Difesa Civile
Prefetto Laura Lega

Al Capo del Corpo dei Vigili del Fuoco
Ing. Guido Parisi

Al Direttore Centrale per le Risorse Umane
Dipartimento Vigili del fuoco, Soccorso Pubblico e Difesa Civile
Prefetto Fabio Marsilio

Al Direttore Centrale per l'Emergenza, il Soccorso tecnico e l'AIB
Dipartimento Vigili del fuoco, Soccorso Pubblico e Difesa Civile
Ing. Marco Ghimenti

Al Direttore Centrale per la Formazione
Dipartimento Vigili del fuoco, Soccorso Pubblico e Difesa Civile
Ing. Gaetano Vallefuoco

All'Ufficio III Relazioni Sindacali
Dipartimento Vigili del fuoco, Soccorso Pubblico e Difesa Civile
Viceprefetto Bruno Strati

Al Sottosegretario di Stato per l' Interno
On. Carlo Sibilia

Oggetto: **Formazione Personale Ruolo Tecnico Informatico del CNVVF.**

Riceviamo da parte di iscritti e simpatizzanti segnalazioni circa una cronica mancanza di attenzione in merito alla formazione del personale tecnico informatico del Corpo nazionale.

Più precisamente, nonostante i ripetuti appelli e gli innumerevoli suggerimenti espressi in diverse sedi, la formazione del personale tecnico informatico sembra davvero essere ferma ormai da troppo tempo. Le tecnologie informatiche necessitano di un percorso formativo costante all'altezza dei rapidi cambiamenti del mondo I.C.T. (Information Communication Technology) ed a breve vi saranno ulteriori assunzioni di personale, a cui vengono richieste ampie conoscenze ai fini dell'ingresso in ruolo e che, salvo cambiamenti, saranno destinate al non aggiornamento di quanto chiesto in sede concorsuale con possibili ripercussioni negative in un "mondo" (quello del digitale) in rapidissima evoluzione. Eppure lo stesso Piano Nazionale di Ripresa e Resilienza (PNRR) ritiene strategiche la digitalizzazione e l'informatizzazione della Pubblica amministrazione tanto da prevedere, entro il 2026, il transito dell'uso dei servizi in cloud per circa il 75% delle P.A.

È altresì necessario valutare il cambiamento del paradigma formativo offrendo agli informatici del Corpo nazionale tutti gli strumenti e le conoscenze (supportate da idonee certificazioni) necessari per operare e per interfacciarsi pure con enti ed aziende esterni (tra cui corsi di "Cybersecurity") al fine di garantire le migliori soluzioni ed innovazioni nel pieno interesse del CNVVF e quindi del soccorso.

Oltre a ciò la mancanza di corsi di formazione determina un danno anche alle progressioni di carriera di tale personale.

Ciò premesso la scrivente O.S. CO.NA.PO. chiede la tempestiva istituzione di un tavolo tecnico per l'aggiornamento ed il potenziamento formativo del personale tecnico-informatico.

In attesa di cortese riscontro, si ringrazia anticipatamente e si porgono distinti saluti.

Il Segretario Generale aggiunto
CONAPO Sindacato Autonomo VVF
Marco Piergallini

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Alle Direzioni Centrali del Dipartimento dei Vigili del fuoco del soccorso pubblico e della difesa civile

Alle Direzioni Regionali ed Interregionali dei Vigili del fuoco del soccorso pubblico e della difesa civile

Ai Comandi dei Vigili del Fuoco

E p.c. Agli Uffici di diretta collaborazione con il Capo Dipartimento

Agli Uffici di diretta collaborazione con il Capo del Corpo Nazionale dei VVF

OGGETTO: Informativa sicurezza informatica 02/2022 - Nobelium.

Si porta a conoscenza quanto segnalato dalle autorità competenti in sicurezza informatica, in merito ad una recente campagna di attività informatica malevola, che risulterebbe attiva almeno dal 18 gennaio us, congegnata per indurre l'utente vittima ad eseguire il download di un file immagine .ISO/IMG malevolo, per mezzo di un allegato HTML.

Il file IMG/ISO malevolo contiene al suo interno due distinti file, il primo denominato "trello.dll" che rappresenta il first-stage del malware ed un secondo di estensione .LNK, responsabile dell'esecuzione del file.

Si ipotizza che la campagna possa essere collegata alle attività del Threat Actor pubblicamente noto come Nobelium.

Nel dettaglio all'interno della libreria "trello.dll", l'attaccante sfrutta la nota suite di applicazioni Trello e le sue API per simulare un server C2, usato per tener traccia delle vittime e per scaricare un nuovo payload; tra le informazioni inviate dall'attaccante al server si trovano lo username, il nome macchina e l'indirizzo IP interno della vittima.

Al fine di prevenire le suddette attività malevole, risulta urgente innalzare i livelli di attenzione, prendendo le opportune precauzioni al fine di ridurre i rischi cyber.

Nel dettaglio, risulta opportuno intraprendere le seguenti azioni prioritarie da attuare con immediatezza all'interno delle proprie strutture:

- verificare sui log del server proxy della sede la presenza di tentativi di connessione verso i domini identificati come malevoli:
  - petslifenews[.]com
  - tsubux[.]com
  - maybyrne.co[.]uk

- eseguire una scansione sui PC, anche con l'ausilio di Antivirus, per ricercare evidenze di di una eventuale compromissione, utilizzando come ricerca i nomi dei programmi identificati come malevoli:
    - javafx_font.dll
    - trello.dll
- allertare il CED Dipartimento in caso di riscontro positivo;
- innalzare il livello di protezione delle credenziali utente ed amministrative, implementando, ove non già presenti, sistemi di autenticazione a più fattori.

Pertanto, si richiede al personale informatico di verificare, per quanto di propria competenza, la presenza della libreria in oggetto, in dispositivi presenti in sede.

In caso di riscontro positivo, si prega di isolare dalla rete la postazione infetta ed implementare le contromisure di sanitizzazione e di notificare eventuali evidenze di compromissione allo scrivente Ufficio.

Si confida nella collaborazione di codesti Uffici nell'attuazione delle misure di sicurezza indicate, che possono innalzare in modo significativo l'efficacia delle misure di prevenzione attuate dallo scrivente Ufficio e delle misure di monitoraggio continuo attuate dal CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).

IL DIRIGENTE
(Dott.Ing. Davide POZZI)
(documento firmato digitalmente ai sensi di legge)

POZZI DAVIDE
MINISTERO
DELL'INTERNO/80219290584
26.01.2022 18:29:03 GMT+01:00

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Alle Direzioni Centrali del Dipartimento dei Vigili del fuoco del soccorso pubblico e della difesa civile

Alle Direzioni Regionali ed Interregionali dei Vigili del fuoco del soccorso pubblico e della difesa civile

Ai Comandi dei Vigili del Fuoco

E p.c. Agli Uffici di diretta collaborazione con il Capo Dipartimento

Agli Uffici di diretta collaborazione con il Capo del Corpo Nazionale dei VVF

OGGETTO: Informativa sicurezza informatica 01/2022 – Vulnerabilità Log4Shell.

Si porta a conoscenza del personale informatico degli Uffici in indirizzo che Apache Software Foundation ha rilasciato un avviso che notifica alcune vulnerabilità, di cui una zero-day critica con PoC dell'exploit già pubblicato, nella libreria Java Log4j.

Log4j è una libreria Java inclusa in moltissimi framework Apache, tra cui Struts2, Solr, Druid e Flink. ed è presente in numerosi progetti open-source come Redis, ElasticSearch, Elastic Logstash e Ghidra.

Log4j viene utilizzata nelle applicazioni java-based per la scrittura degli eventi applicativi nei file di log sul sistema in cui è in esecuzione, infatti, è largamente utilizzata nello sviluppo di sistemi aziendali, ed è inclusa in vari software open-source e spesso direttamente integrata in importanti applicazioni software.

Data la natura multipiattaforma di Java, il fronte di attacco interessa una moltitudine di sistemi di diversa architettura (Windows, Linux, dispositivi di vario genere, micro-servizi, cloud, etc).

Quindi, si richiede al personale informatico di verificare, per quanto di propria competenza, la presenza della libreria in oggetto, in dispositivi presenti in sede o in applicazioni sviluppate in autonomia, che siano installate all'interno della rete del Dipartimento.

In caso di riscontro positivo, si prega di attuare le contromisure riportate nell'allegato, o di seguire le istruzioni pubblicate da Apache Software e <u>di notificare eventuali evidenze di compromissione allo scrivente Ufficio</u>.

Si coglie l'occasione per richiamare l'attenzione di tutto il personale riguardo l'utilizzo di apparati e strumentazioni informatiche non fornite dall'Amministrazione, che dovranno essere connesse sempre sotto la supervisione del personale informatico della sede. Si rammenta che è vietato collegare router

WiFi nella rete del Dipartimento, che stabiliscono connessione Internet tramite SIM telefonica, che possano creare conflitti in rete o addirittura possibilità di accesso non autorizzato alla LAN della sede.

Si confida nella collaborazione di codesti Uffici nell'attuazione delle misure di sicurezza indicate, che possono innalzare in modo significativo l'efficacia delle misure di prevenzione attuate dallo scrivente Ufficio e delle misure di monitoraggio continuo attuate dal CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).

IL DIRIGENTE
(Dott. Ing. Davide POZZI)
(documento firmato digitalmente ai sensi di legge)

POZZI DAVIDE
MINISTERO
DELL'INTERNO/80219290584
26.01.2022 18:29:03
GMT+01:00

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Indicazioni tecniche Vulnerabilità Log4Shell

La vulnerabilità è stata denominata Log4Shell, e identificata con codice CVE-2021-44228 e indice di gravità CVSS 10.0, sfruttabile da attaccanti non autenticati, che consente la totale compromissione del sistema.

Data la natura multipiattaforma di Java, il fronte di attacco interessa una moltitudine si sistemi di diversa architettura (Windows, Linux, dispositivi di vario genere, micro servizi, cloud, etc).

La vulnerabilità è di livello critico, in quanto permette l'esecuzione di codice arbitrario da remoto (RCE) senza nessuna autenticazione sul sistema che utilizza la libreria, per cui un malintenzionato ha la possibilità di inviare una richiesta http o https malformata e costruita appositamente con una stringa formattata e contenete parametri tali da indurre la libreria a generare un log su Log4j, che adotta JNDI (Java Naming and Directory Interface), al fine di scrivere la stringa dannosa nel log dell'applicazione. Durante l'elaborazione del log, il sistema vulnerabile esegue il codice inserito dall'utente malintenzionato, che generalmente punta a scaricare da server esterni da esso controllati, il codice malevolo che potrà essere eseguito svolgendo il compito per cui è stato creato, ottenendo quindi il controllo remoto del server (RCE).

Dalle indagini effettuate le richieste verso i server utilizzano i protocolli LDAP e DNS.

I tentativi di attacco possono essere individuati nei log generati da Log4j dalla presenza di "jndi" (che si riferisce alla Java Naming and Directory Interface) e dal fatto che il protocollo di comunicazione "ldap", "ldaps", "rmi", "dns", "iiop", o "http" precede il dominio dell'avversario.

Lista non esaustiva applicazioni che utilizzano Log4j

- Elastic Search
- Elastic LogStash
- GrayLog2
- Minecraft (client and server)
- Neo4J
- Progetti Apache (Druid, Dubbo, Flink, Flume, Hadoop, Kafka, Solr, Spark, Struts, Tapestry, Wicket)
- Prodotti VMware (Horizon, vCenter, vRealize, HCX, NSX-T, UAG, Tanzu)
- Grails
- prodotti java custom
- altro.
- Applicazioni Java custom
- Dispositivi di rete come stampanti, ip cam

Le versioni interessate dalla vulnerabilità CVE-2021-44228 sono dalla 2.0-beta9 fino a 2.12.1 e da 2.13.0 a 2.15.0

Apache ha rilasciato la versione 2.16 per risolvere la vulnerabilità.

Ministero dell'Interno

DIPARTIMENTO DEI VIGILI DEL FUOCO E DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVILE
DIREZIONE CENTRALE PER LE RISORSE LOGISTICHE E STRUMENTALI
Ufficio per le Tecnologie dell'Informazione e della Comunicazione

Venerdì 17 dicembre l'Apache Software Foundation ha rilasciato la versione 2.17.0 della libreria Log4j per correggere una terza vulnerabilità identificata con codice CVE-2021-45105 (CVSS 7.5), che impatta tutte le versioni dalla 2.0-beta9 alla 2.16.0 e può causare sul sistema un DoS (Denial of Service).

Se la configurazione di logging utilizza un Pattern Layout non predefinito con un Context Lookup (ad esempio, $${ctx:loginId}), un attaccante con il controllo sui dati di input Thread Context Map (MDC) può creare imput malevoli conteneti un lookup ricorsivo causando uno StackOverflowError che termina il processo.

I suggerimenti per mitigare CVE-2021-45105 sono i seguenti: in Pattern Layout nella configurazione di logging, sostituire i Context Lookups (come ${ctx:loginId} o $${ctx:loginId}) con i pattern Thread Context Map (%X, %mdc, o %MDC), oppure rimuovere i riferimenti ai Context Lookup (come ${ctx:loginId} o $${ctx:loginId}) quando provengono da fonti esterne all'applicazione come gli header HTTP o l'input dell'utente.

Se non è possibile applicare le patch, si consiglia vivamente di isolare il sistema da Internet e/o di applicare le seguenti misure di mitigazione:

Per la versione >=2.10: impostare log4j2.formatMsgNoLookups a "true";

Per le versioni dalla 2.0 alla 2.10.0: si può rimuovere completamente la classe LDAP da log4j eseguendo il seguente comando:

"*zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class;*"

Controllare i tentativi di sfruttamento su sistemi Linux/Unix nei log del server web usando il seguente comando:

"*sudo egrep -i -r '\${jndi:(ldap[s]?|rmi|dns):/[^\n]+' /var/log/;* "

Tra i primi a subire le conseguenze dei tentativi di exploitation c'è stata la piattaforma di gaming Minecraft di Microsoft.

Al momento risultano potenzialmente impattate soluzioni di numerosi vendor tra cui: Akamai, Apache, Atlassian, Amazon,Apple, BitDefender, Broadcom, Cisco, Citrix, CheckPoint, Cloudflare, CPanel, Debian, Dell, ESET, Elastic, F5 Networks, Fortinet, GitHub, Ghidra, Google, IBM, Jboss, Jenkins, Jitsi, McAfee, Microsoft, Minecraft, MISP, Netflix, Oracle, Pulse Secure, SAP, SolarWinds, SonicWall, Sophos, TrendMicro, Ubuntu, VMware, Yandex e ZSCALER.

Per ulteriori informazioni di dettaglio si rimanda ai siti dei produttori.

Fonti:
https://logging.apache.org/log4j/2.x/security.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228