Basque CyberSecurity Centre

Zero-day ahultasunak Microsoft Exchange-n

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako, BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiatzea, banatzea, hedatzea edo ezagutzera ematea.

BCSC-ri buruz

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Laburpen exekutiboa

Microsoften Segurtasun Erantzunen Zentroko taldeak argitalpen bat egin du zero day-ko bi ahultasunen inguruan, eta GTSC izeneko Vietnamgo segurtasun-taldeak hasiera batean jakinarazi ditu.

Microsoftek nabarmendutako lehen ahultasuna CVE-2022-41040 sisteman dago identifikatuta. Horren bidez, zerbitzariaren aldeko eskaera-eraso faltsu bat egin daiteke (SSRF). Hala ere, CVE-2022-41082 sisteman jarraitutako bigarren akatsak urruneko erasotzaile bati kode arbitrarioa urrunetik exekutatzeko aukera ematen dio (RCE).

Konpainiak bi ahultasunen ustiapenari buruz dagoen ezagutza nabarmendu du, Microsoft Exchange zerbitzari ahulerako sarbide baimendua izateko beharra aipatuz. Ahultasun horiek baliatzen dituzten zuzendutako erasoetan, lehenik eta behin CVE-2022-41040 akatsa exekutatzen da, erasotzaileek urrunetik aprobetxa baitezakete CVE-2022-41082 sisteman deskribatutako akatsa.

Oraingoz, ez da aurkitu ahultasun horiek aprobetxatzen dituen inolako exploit edo kontzeptu-probarik (PoC) argitaratu denik.

Gaineratu behar da oraingoz ez dela aplikatu deskribatutako akatsak konponduko dituen irtenbide ofizialik, baina Microsoftek eta GTSCk ordezko arintzeak argitaratu dituzte. BCSCk ahalik eta azkarren aplikatzea gomendatzen du, ahultasun horiek kritikotzat jotzen dira kaltetutako sistema ahulen konpromisoa saiheste aldera.

.

2. Azterketa teknikoa

Duela gutxi egindako aurkikuntzaren ondorioz, oraingoz ez dago informazio nahikorik CVE-2022-41040 eta CVE-2022-41082 ahultasunen xehetasun osoa ezagutzeko. Jarraian, bi akatsen orain arte ezagututako xehetasun teknikoak nabarmenduko ditugu:

- CVE-2022-41040: Erabiltzaileak Exchange OWA interfazean emandako sarreraren balioztatze eskasaren ondorioz dagoen ahultasuna. Urruneko erabiltzaile batek bereziki diseinatutako HTTP eskaera bidal dezake, eta aplikazioa engainatu, sistema arbitrarioetarako eskaerak has ditzan. Urrakortasun hori arrakastaz ustiatuta, urruneko erasotzaile batek kode arbitrarioa exekutatu dezake helburu-sisteman.
- CVE-2022-41082: Sarbide desegokiko balioztatze baten ondorioz sortutako ahultasuna. Urruneko erabiltzaile batek Exchange sistema ahuletan PowerShell Remoting-erako sarbidea badu, kode arbitrarioa exekutatu dezake.

Aurrekoaz gain, GTSCk ezagutarazi ditu Exchange zerbitzari ahulen konpromisoak atzemateko metodoak, baita zibererasotzaileek erabilitako konpromiso-adierazleak ere (IOC´s) zero-day ahultasunak aprobetxatzen dituztenak.

Zerbitzari baten balizko konpromiso bat bilatzeari dagokionez, GTSCk PowerShell komando hau exekutatzea gomendatzen du, IIS fitxategiak eskaneatzeko, konpromiso-adierazleen bila:

- *Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200*

Deskribatutako ahultasunetan antzemandako konpromiso-adierazleak (IOC´s) esteka honetan deskarga daitezke:

- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

Azpimarratu behar da horiek aztertu ondoren, ahultasun hori ustiatzen duten erasotzaileen jatorria asiarra dela, Chopper-en webshell-ak aplikatzen baitituzte.

Amaitzeko, eragindako baliabideak nabarmenduko ditugu:

- Microsoft Exchange Server 2013, 2016 y 2019.

3. Arintzea / Konponbidea

Ohiko moduan, ahultasun hori eta beste batzuk saihesteko, BCSCk gomendatzen du sistemak eta aplikazioak beti eguneratuta izatea eskura dagoen azken bertsiora, dagozkion adabakiak argitaratu bezain laster.

Garrantzitsua da neurriak azkar hartzea, ezarpenaren arazoa arintzeko. Oraingoz ez da partxe ofizialik argitaratu, baina bai Microsoftek bai GTSCk jakinarazi dute aplikatu beharreko arintze alternatiboa.

Lehenik eta behin, Microsoft Exchange Online erabiltzen duten erabiltzaileek ez dutela ezer egin behar adierazten du. Hala ere, Microsoft Exchange modu lokalean erabiltzen dutenek URL berridazteko hainbat jarraibide aplikatu behar dituzte, eta erakutsi zaizkien PowerShell-eko urruneko atakak blokeatu.

Horretarako, administratzaileek blokeo erregela bat gehitu behar dute *"ISSren administratzailean" > Aurrez zehaztutako webgunea > Detekzio automatikoa > URLren berridazketa > Ezagutzen diren eraso ereduak blokeatzeko ekintzak.*

Adierazitako urratsak egin ondoren, ezaugarrien ikuspegiaren barruan *URL berridazketan* sartu behar da. Ondoren, arauak gehitu behar dira ekintza-panelean. Ondoren, blokeoa eskatu, kate hau gehituta:

- *.*autodiscover\.json.*\@.*Powershell.**

Urrats hori egin ondoren, lehen sortutako araua zabaldu eta baldintzak editatu behar dira, eta sarrera-baldintza aldatu egin behar da: *{URL}* -etik *{REQUEST_URI}*-ra.

4. Erreferentzia osagarriak

- Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server.
- Warning: New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server.
- MITRE: CVE-2022-41040.
- CWE-918: Server-Side Request Forgery (SSRF).
- MITRE: CVE-2022-41082.
- CWE-94: Improper Control of Generation of Code ('Code Injection').
- CWE-20: Improper Input Validation.
- Outlook en la web en Exchange Server.
- Connect to Exchange servers using remote PowerShell.
- https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- MITRE: China Chopper.

Basque CyberSecurity Centre

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA