REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO
UPRAVA REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 47 78
E: gp.uiv@gov.si
W: www.uiv.gov.si

Medijem po adremi

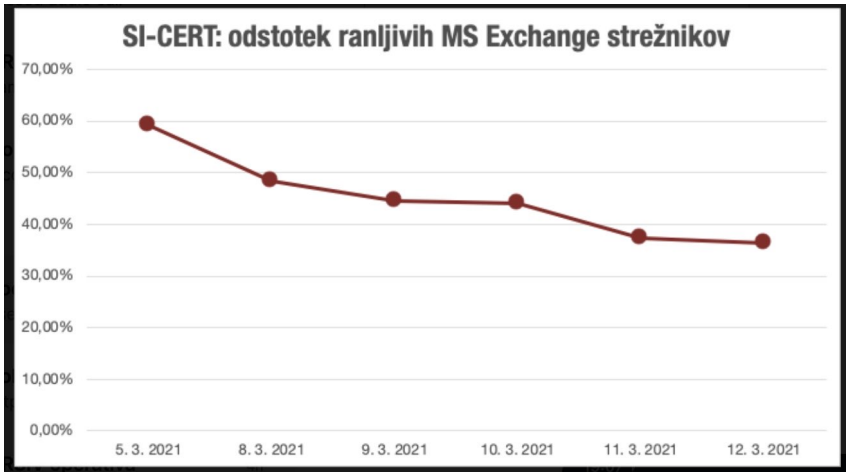
Številka: 091-1/2020-3132-24

Datum: 15.3.2021

Zadeva: SPOROČILO ZA JAVNOST: **KRITIČNE RANLJIVOSTI MICROSOFT EXCHANGE STREŽNIKOV**

Podjetje Microsoft je 3. marca 2021 zjutraj (po sredjeevropskem času) objavilo, da v njihovem izdelku **Microsoft Exchange Server**, enemu od najbolj razširjenih strežnikov za elektronsko pošto, vodenje koledarjev in stikov ter sodelovanje, obstaja **več kritičnih ranljivosti**. Navedeno pomeni, da strežnik Exchange Server vsebuje hude napake, ki se lahko izkoristijo za **krajo informacij (tudi zbirk osebnih podatkov), šifriranje podatkov za izsiljevanje/odkupnino, posledice pa so za organizacijo lahko zelo resne in povzročijo daljši izpad poslovanja**. Ogrožena so tudi omrežja v katera so ti strežniki priključeni. Zato je te strežnike potrebno **čimprej popraviti** tako, da se nanje namestijo ustrezni popravki. Več podrobnosti ter navodila v slovenskem jeziku so objavljena na spletnih straneh Uprave RS za informacijsko varnost (URSIV) ter nacionalnega odzivnega centra za kibernetsko varnost (SI-CERT) (http://uiv.gov.si/ in https://www.cert.si/si-cert-2021-01/).

Odprava kritičnih ranljivosti Microsoft Exchange serverjev v Sloveniji je ponekod **sorazmerno počasna**, še posebej v manjših podjetjih. Zato URSIV, kot pristojni nacionalni organ za informacijsko varnost, skupaj s SI-CERT - nacionalnim odzivnim centrom za kibernetsko varnost, **poziva vse lastnike in upravljalce Microsoft Exchange Server strežnikov v Sloveniji, da poskrbijo za varnost svojih organizacij**, zaposlenih, poslovnih partnerjev in drugih tako, da **čim prej nadgradijo svoje Microsoft Exchange strežnike z uradno izdanimi popravki**.



Vir: SI-CERT

Delež ranljivih Microsoft Exchange strežnikov v Sloveniji je še vedno zelo visok in stagnira. **Posebno opozorilo velja skrbnikom in vodstvom malih in srednjih podjetij**, ki naj čim prej namestijo popravke oz. se obrnejo po pomoč na SI-CERT (cert@cert.si), da ne bodo postali žrtve izsiljevalskih napadov. Navodila SI-CERT so skrbniki omrežij, v katerih se ranljivi strežniki nahajajo, že prejeli.

Glede na resnost razmer je URSIV, v skladu z 22. členom Zakona o informacijski varnosti (ZInfV), **razglasila stanje povečane ogroženosti varnosti omrežij ali informacijskih sistemov**. URSIV ima po ZInfV pristojnosti nad zavezanci po tem zakonu, ki so organi državne uprave, izvajalci bistvenih storitev in ponudniki digitalnih storitev. Zavezancem lahko, v skladu z zakonodajo, nalaga ukrepe za zmanjšanje informacijskih in kibernetskih varnostnih tveganj ter inšpekcijsko preverja. Za ostale, ki niso zavezanci po ZInfV, URSIV objavlja to sporočilo za javnost in prosi medije za podporo oz. hitro in ustrezno objavo teh zelo pomembnih informacij.

URSIV dodatno pojasnjuje, da zgoraj navedene kritične ranljivosti ne ogrožajo drugih sistemov elektronske pošte.

Podrobneje o kritičnih ranljivostih MS Exchange strežnikov, postopkih za odpravo le teh ter situaciji v Sloveniji

Kritične ranljivosti so vrste “Microsoft Exchange Server Remote Code Execution Vulnerability” podrobneje opisane v CVE-2021-26855[1], CVE-2021-26857[2] in CVE-2021-26858[3], CVE-2021-27065[4]. Izkoriščanje verige teh kritičnih ranljivosti Microsoft Exchange Serverja napadalcem omogoča dostop do predalov elektronske pošte in namestitev škodljive programske opreme na ranljivi MS Exchange strežnik ter potencialno tudi dostop do drugih informacijskih sistemov na omrežju organizacije. Obstaja verjetnost, da so zlonamerni akterji te ranljivosti izkoriščali že od septembra 2020. Veriženje kritičnih ranljivosti napadalcem omogoča dostop do predalov elektronske pošte in namestitev škodljive programske opreme na ranljivi MS Exchange strežnik.

Podjetje Microsoft je 2. marca 2021, hkrati z objavo informacije o kritičnih ranljivostih, pripravilo tudi popravke, ki jih je potrebno namestiti na Microsoft Exchange strežnike. Prizadeti so strežniki Exchange Server 2013, Exchange Server 2016 in Exchange Server 2019 pa tudi Exchange Server 2010[5]. Ena od

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26857
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26858
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27065
[5] https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

kritičnih ranljivosti namreč velja tudi za ta izdelek, ki sicer ni več vzdrževan. Microsoft je, kot začasno rešitev, vseeno objavil popravek.

SI-CERT - nacionalni odzivni center za kibernetsko varnost - je 3. marca objavil varnostno obvestilo SI-CERT 2021-01[6] v katerem je opisal ranljivosti Microsoft Exchange strežnikov ter podal preventivne ukrepe, ki se nanašajo na namestitev popravkov, pregled indikatorjev zlorabe in ukrepe pri zaznani zlorabi. O ranljivosti so bili takoj obveščeni vsi izvajalci bistvenih storitev. Temu je sledil pregled slovenskega internet prostora z namenom identifikacije ranljivih strežnikov, sporočila o ranljivosti in ustreznih ukrepih pa so bila razposlana skrbnikom omrežij 8. in zopet 12. marca.

URSIV kot pristojni nacionalni organ za informacijsko varnost pozorno spremlja razvoj dogodkov. Na podlagi preliminarne analize SI-CERT, ki kaže na razširjenost potencialno ranljivih strežnikov v Republiki Sloveniji, URSIV sklepa, da obstaja povečana ogroženost varnosti omrežij in informacijskih sistemov pri izvajalcih bistvenih storitev različnih sektorjev in organih državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti in ki uporabljajo Exchange strežnike. URSIV prav tako ocenjuje, da so lahko ogroženi tudi upravljalci kritične infrastrukture.

Zaradi navedenega je URSIV 6. marca 2021 pozvala SIGOV-CERT - odzivni center za incidente v informacijskih sistemih organov državne uprave ter Nacionalni center za krizno upravljanje (NCKU), da tako državne organe kot tudi upravljalce kritične infrastrukture pozovejo k takojšnji odpravi ranljivosti, če tega še niso storili. Prav tako je URSIV pozval SIGOV-CERT in NCKU k rednemu poročanju v zvezi z zaznavanjem in/ali odpravo prej omenjenih ranljivosti.

URSIV je 7. marca 2021 ocenil, da je nastopilo stanje povečane ogroženosti varnosti omrežij in informacijskih sistemov zavezancev po Zakonu o informacijski varnosti, ki so bili s sklepom Vlade Republike Slovenije na podlagi navedenega zakona določeni kot izvajalci bistvenih storitev oziroma organi državne uprave.

V skladu s svojimi pristojnostmi je URSIV 8. marca 2021 izdal odločbe izvajalcem bistvenih storitev, s katerimi jim je naložil ustrezne ukrepe v povezavi s prej omenjenimi kritičnimi ranljivostmi.

URSIV meni, da stanje povečanje ogroženosti varnosti omrežij in informacijskih sistemov velja tudi za druge organizacije v Republiki Sloveniji, ki uporabljajo Microsoft Exchange strežnike zgoraj navedenih verzij. Zaradi tega **URSIV vsem, ki imajo v lasti ali upravljanju Microsoft Exchange strežnike priporoča, da skrbno spremljajo obvestila SI-CERT in ostalih (predvsem Microsoft) v zvezi z zgoraj navedenimi kritičnimi ranljivostmi ter da ustrezno poskrbijo za namestitev popravkov ter za pregled indikatorjev zlorab.** URSIV vse skrbnike Microsoft Exchange strežnikov prosi, da morebitne zaznane zlorabe prostovoljno sporočijo na SI-CERT (cert@cert.si).

Mediji nas lahko za več informacij kontaktirate na gp.uiv@gov.si in press@cert.si.

S spoštovanjem,

Gorazd Božič
Vodja SI-CERT

Dr. Uroš Svete
Direktor Uprave RS za informacijsko varnost

[6] https://www.cert.si/si-cert-2021-01/