



Kyberkatsaus

09/2026

LOIHDE



Tiivistelmä

Syyskuun kyberkatsauksessa on nostettu esille kiinnostavia poimintoja ajankohtaisista tapahtumista kyberkentällä:

- Usean eri laitevalmistajan reunalaitteissa on ollut syyskuussa kriittisiä, aktiivista hyväksikäyttöä kohdanneita tietoturva- haavoittuvuuksia
- JadePuffer:ksi nimetty kiristyshaittaohjelmatoimija on suorittanut hyökkäyksiä Azure-resursseihin
- Tietoturvatestauksessa käytettyjä AI-agentteja on murtautunut tuotantojärjestelmiin testivaiheessa
- Syyskuun suositukset kohdistuvat reunalaitteiden haavoittuvuuksiin liittyvien tiedotteiden seuraamiseen, korjaustoimenpiteisiin ja mahdollisten murtojen havaitsemiseen



Kriittisiä haavoittuvuuksia eritoten verkon reunalaitteissa

Syyskuun kyberkatsaus tiivistää sen, mistä Loihteen CSOC on kirjoittanut koko vuoden: Organisaation julkiverkkoon näkyvät reunalaitteet ovat uhkatoimijoiden ensisijainen sisään tuloreitti. Useita näitä haavoittuvuuksia yhdistää se, että niitä on hyväksikäytetty jo haavoittuvuuden julki tullessa tai sitä ennen.



Reunalaitteet ovat jatkuvasti alttiita tietomurroille, eikä esim. IP-rajauksia voida hyödyntää kaikissa järjestelmissä.



Tarvitaan selkeä suunnitelma ja prosessi haavoittuvuuksien nopeaan paikkaamiseen ja tietomurtojen havaitsemiseen.

Loihteen CSOC:n suositukset

1

Nimeä haavoittuvuustiedotteiden seurannalle vastuhenkilö ja varahenkilö, jotka reagoivat tiedotteisiin saman päivän aikana

2

Määrittele ja harjoittele hätäpäivitysprosessi, joka ohittaa normaalin huoltoikkunan

3

Tarkista päivityksen jälkeen mahdolliset murron merkit, sillä päivitys ei välttämättä poista jo saatua jalansijaa

KUUKAUSIRAPORTTI 09/2026

Tämä raportti sisältää poimintoja syyskuun 2026 kybertapahtumista. Raportin sisältö pohjautuu avoimiin lähteisiin, joita ovat esimerkiksi uutiset, sosiaalisen median palvelut ja muut aiheeseen liittyvät verkkolähteet. Raportti tuo esille kyberturvallisuuteen liittyviä merkittäviä tapahtumia ja trendejä, jotka vaikuttavat meidän ja asiakkaidemme toimintaan.

Sisällys

Tiivistelmä	1
KUUKAUSIRAPORTTI 09/2026	2
1. Poiminnat	3
1.1 AI agenttien testivaiheessa tekemät kyberhyökkäykset	3
1.2 Syyskuun aikana useita kriittisiä haavoittuvuuksia verkon reunalaitteissa	4
1.3 Citrix Netscaler ADC ja Gateway CVE-2026-88771, CVE-2026-88772	4
1.4 JadePuffer kiristyshaittaohjelmatoimija Azuressa	5
2. Suositukset	6

1. Poiminnat

1.1 AI agenttien testivaiheessa tekemät kyberhyökkäykset

Kesän aikana on raportoitu useista tapauksista, jossa testausvaiheessa ollut tekoälymalli on karannut testistä ja hyökännyt oikeita kohteita kohtaan. Ensimmäinen raportoitu tapaus oli OpenAI GPT 5.6 Sol-kielimallin ja toisen nimeämättömän kielimallin hyökkäys Hugging Face-yhtiön infrastruktuuriin. Kyseisiä kielimalleja käyttävät agentit olivat tekemässä ExploitGym¹-tietoturvatestiä, jonka aikana ne keksivät Hugging Face:lla mahdollisesti olevan vastaukset testiin ja päättivät yrittää varastaa niiden vastaukset.²

OpenAI:n jälkeen mm. Anthropic³, Meta⁴ ja Google⁵ ilmoittivat omien agenttiensa murtautuneen luvattomasti eri organisaatioiden järjestelmiin. Tapaukset vaihtelevat yksinkertaisesta Internetistä löytyneen tunnuksen kokeilusta kohdejärjestelmään laajempiin Hugging Facen kaltaisiin murtautumisiin. Useat tapaukset on yhdistetty Irregular-nimiseen yritykseen, joka tarjoaa testauspalveluita AI-kehittäjille. Irregular julkisti tiedotteen elokuussa, jossa vahvistaa testialustassa olleen konfiguraatiovirheen mahdollistaneen agenttien karkaamiset julkiverkkoon⁶.

Viimeisimpänä OpenAI ilmoitti peruvansa tulevan GPT 6.1 Astra -mallin julkaisun testivaiheessa löytyneiden ongelmien vuoksi. Asiasta raportoiva WSJ ei tarkemmin mainitse kyseessä olleen kyberliitännäisiä ongelmia, mutta yleisesti malli koitti tehdä toimia, johon sillä ei ollut lupaa⁷. Tätä ennen OpenAI ilmoitti tapauksesta, jossa agentti löysi tavan kommunikoida testialustalta julkiverkkoon DNS-tunneloinnin avulla, jonka seurauksena löydettyjen ongelmien vuoksi OpenAI on lopettanut väliaikaisesti kaikkien kehittyneimpien mallien koulutuksen⁸.

¹ExploitGym, N.d. <https://github.com/sunblaze-ucb/exploitgym>

² OpenAI, OpenAI – Hugging Face Incident, <https://cdn.openai.com/pdf/67869394-cb91-4c12-888c-5cbd85c7814c/OpenAI-Hugging-Face%20Incident-Technical-Report.pdf>

³ Anthropic, 30.7.2026, Investigating three real-world incidents in our cybersecurity evaluations, <https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals>

⁴ Reuters, 5.8.2026, Meta AI model hacks another company during testing, <https://www.reuters.com/technology/metas-ai-model-hacked-another-company-during-testing-information-reports-2026-08-05/>

⁵ BBC, 19.9.2026, Google's Gemini AI hacked three companies in security test, <https://www.bbc.com/news/articles/c60710k72rlvo>

⁶ Irregular, 14.8.2026, Addressing Recent Incidents: Ongoing Findings and Path Forward, <https://www.irregular.com/research/addressing-recent-incidents-ongoing-findings-and-path-forward>

⁷ WSJ, 28.9.2026, OpenAI Scraps Release of New AI Model Over Safety Concerns, <https://www.wsj.com/tech/ai/openai-chatgpt-model-release-cancel-safety-5a2f9f42>

⁸ OpenAI, 25.9.2026, An agent used DNS to reach an external chatbot, <https://alignment.openai.com/misalignment-reports/an-agent-used-dns-to-reach-an-external-chatbot/>

1.2 Syyskuun aikana useita kriittisiä haavoittuvuuksia verkon reunalaitteissa

Syyskuussa julkistettiin kriittisiä tietoturva- haavoittuvuuksia usean eri valmistajan verkon reunalaitteeseen. Näitä edustivat mm. Citrix NetScalerin haavoittuvuudet CVE-2026-88771 ja CVE-2026-88772, F5 BIG-IP APM:n CVE-2026-94127, Cisco ISE CVE-2026-76423, Cisco Secure Email Gateway CVE-2026-76461 ja SonicWall SMA1000 CVE-2026-83548 sekä CVE-2026-83549.⁹¹⁰¹¹¹²

Kaikkia näitä haavoittuvuuksia yhdistää se, että niitä on hyväksikäytetty jo haavoittuvuuden julki tullessa tai sitä ennen. Tämä muodostaa organisaatioille haastavan tilanteen, koska reunalaitteet voivat joutua koska tahansa alttiiksi tietomurroille eikä esimerkiksi IP-rajauksia voida kohdistaa kaikkiin järjestelmiin. Tällöin pitää olla olemassa suunnitelma ja prosessi sille, kuinka haavoittuvuuksien paikkaamiset voidaan suorittaa nopeasti sekä havaita mahdolliset murrot järjestelmissä.

Citrixin kohdistunutta haavoittuvuutta on avattu tarkemmin seuraavassa osiossa.

1.3 Citrix Netscaler ADC ja Gateway CVE-2026-88771, CVE-2026-88772

Citrix julkaisi 27.9. tiedon useammasta kriittisestä haavoittuvuudesta Netscaler-tuotteisiin, joista kaksi haavoittuvuutta oli julkaisuhetkellä aktiivisesti hyväksikäytön kohteena. Aktiivisesti hyväksikäytetyt haavoittuvuudet ovat CVE-2026-88771 ja CVE-2026-88772. CVE-2026-88772 vaatii Netscalerilla olevan DTLS-konfiguraatio käytössä ja mahdollistaa muistin ylivuodon avulla hyökkääjän ajaa omaa koodia laitteella ilman kirjautumista. CVE-2026-88771 koskee kaikkia Netscalereita konfiguraatiosta riippumatta ja mahdollistaa myös ilman kirjautumista koodin ajamisen laitteella.¹³

CERT-EU on julkaissut blogikirjoituksen CVE-2026-88771 haavoittuvuuden hyväksikäytöstä. Haavoittuvuus toimii kahdessa osassa. Ensiksi haittatoimija tekee HTTPS-kyselyitä käyttäen

⁹ Citrix, 27.9.2026, Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin for CVE-2026-88771 through CVE-2026-88778, https://community.citrix.com/techzone-blogs/110_security-updates/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve-2026-88771-through-cve-2026-88778/

¹⁰ SonicWall, 1.9.2026, Product Notice: SMA 1000 Series affected by Multiple Vulnerabilities (SNWLID-2026-0016), <https://www.sonicwall.com/support/notices/product-notice-sma-1000-series-affected-by-multiple-vulnerabilities-snwlid-2026-0016/kA1VN000002AXmQ0AW>

¹¹ Cisco, 16.9.2026, Cisco Identity Services Engine Vulnerabilities, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ>

¹² Cisco, 14.9.2026, Cisco Secure Email Gateway SQL Injection Vulnerability, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>

¹³ Citrix, 27.9.2026, Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin for CVE-2026-88771 through CVE-2026-88778, https://community.citrix.com/techzone-blogs/110_security-updates/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve-2026-88771-through-cve-2026-88778/

user agenttia, johon on piilotettu haitallinen koodi base64-formaatissa. Tämän jälkeen haittatoimija yrittää hyväksikäyttää haavoittuvuutta Netscalerin kirjautumisessa, joka ajaa aikaisemmin user agenttiin piilotetun koodin. Haavoittuvuuden avulla on yritetty asentaa ainakin webshellejä, jotka mahdollistavat haittatoimijalle koodin ajamisen tietynlaisilla HTTP-kyselyillä.¹⁴

Suosittellemme päivittämään kaikki käytössä olevat Netscalerit mahdollisimman pian. Päivityksen lisäksi suosittelemme käymään kaikki Netscalerit läpi mahdollisen hyväksikäytön varalta. Tämänhetkisten tietojen perusteella ainakin tiedosto `/var/netscaler/logon/LogonPoint/custom/.ctxs.receiver` Netscalerin levyllä on varma merkki haavoittuvuuden hyväksikäytöstä¹⁵. Toinen merkki hyväksikäytöstä on "php_flag engine on" rivi sekä "AddHandler application/x-httpd-php <extension>" konfiguraatio `/etc/httpd.conf` -tiedostossa, jolla konfiguroidaan PHP toimimaan poikkeavilla tiedostopäätteillä¹⁶. On syytä olettaa, ettei päivitys poista jo asennettuja webshellejä, vaan ne täytyy poistaa manuaalisesti.

1.4 JadePuffer kiristyshaittaohjelmatoimija Azuressa

Microsoft Security Research -tiimi raportoi Azureen kohdistuneesta haitallisesta toiminnasta, jossa epäilysti on käytetty AI-agentteja tiedonkeruuseen ja resurssien tuhoamiseen. Epäilty toimija on nimetty JadePuffer:ksi. Microsoft käyttää toimijasta myös nimeä Storm-3168. Pilvipalveluiden tietoturvaan erikoistunut yhtiö Sysdig raportoi JadePuffer-toimijasta alun perin heinäkuussa.¹⁷

Hyökkäyksessä väärinkäytettiin kahta service principalia, joista ensimmäistä oli käytetty ympäristön tiedusteluun ja tiedonkeruuseen. Tiedonkeruu kesti vajaat 16 tuntia. Toisella service principalilla oli tämän jälkeen tuhottu Azure-resursseja. Tunnuksien todennäköisesti saatu haltuun kohdeorganisaation GitHub-repositoriosta, jossa service principalien ID:t sekä secretit ovat olleet julkisesti saatavilla. Hyökkäyksen nopeus ja tapahtumien samanaikaisuus viittaavat siihen, että hyökkäys olisi toteutettu automatisoidusti.

Tuhoamistoimenpiteet kohdistuivat mm. Storage accounteihin, Key Vaulteihin, Function Appeihin, SQL-tietokantoihin ja Recovery-palveluihin. Suurin osa resurssien tuhoamisista onnistui, mutta esimerkiksi osa Storage Accounteista oli suojattu Resource lockeilla ja samanaikaisesti yritetyt SQL-kantojen poistot epäonnistuivat myös uhkatoimijan käyttämän vanhentuneen API-version vuoksi. Tuhoamistoimet suoritettiin seitsemässä minuutissa.

¹⁴ CERT-EU, 28.9.2026, Taking 'execute logging' a bit too literally - CVE-2026-88771, <https://www.cert.europa.eu/blog/taking-execute-logging-a-bit-too-literally-cve-2026-88771>

¹⁵ Greynoise, 28.9.2026, Swarming Against Citrix 0-Day Exploitation, <https://www.greynoise.io/blog/swarming-against-citrix-0-day-exploitation>

¹⁶ Mandiant, 30.9.2026, Defending Against Active Exploitation of Citrix NetScaler ADC and Gateway Appliances, <https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances>

¹⁷ Clark, M. 1.7.2026. JADEPUFFER: Agentic ransomware for automated database extortion. <https://www.sysdig.com/blog/jadepuffer-agentic-ransomware-for-automated-database-extortion>

Tuhoamistoimenpiteiden jälkeen uhkatoimija keräsi jäljelle jääneiden ~30:n Storage Accountien pääsyavaimia ListKeys API-kutsulla, mutta tiedon varastamisesta ei löytynyt viitteitä.

Etenkin tuhoamistoimenpiteet tapahtuivat huolestuttavan nopeasti ja AI-avusteiset hyökkäykset lisääntyvät jatkossa varmasti. Tässä täytyy kuitenkin muistaa se, että hyökkäyspinta-alaa pystytään rajoittamaan merkittävästi noudattamalla tietoturvan perusperiaatteita, eli esimerkiksi käyttöoikeuksien rajaaminen niin ihmis- kuin konekäyttäjiltä sekä niiden säännöllinen katselmointi, salaisuuksien säilyttäminen turvallisissa holveissa (esim. Key Vault) ja näiden kierrättäminen.

2. Suositukset

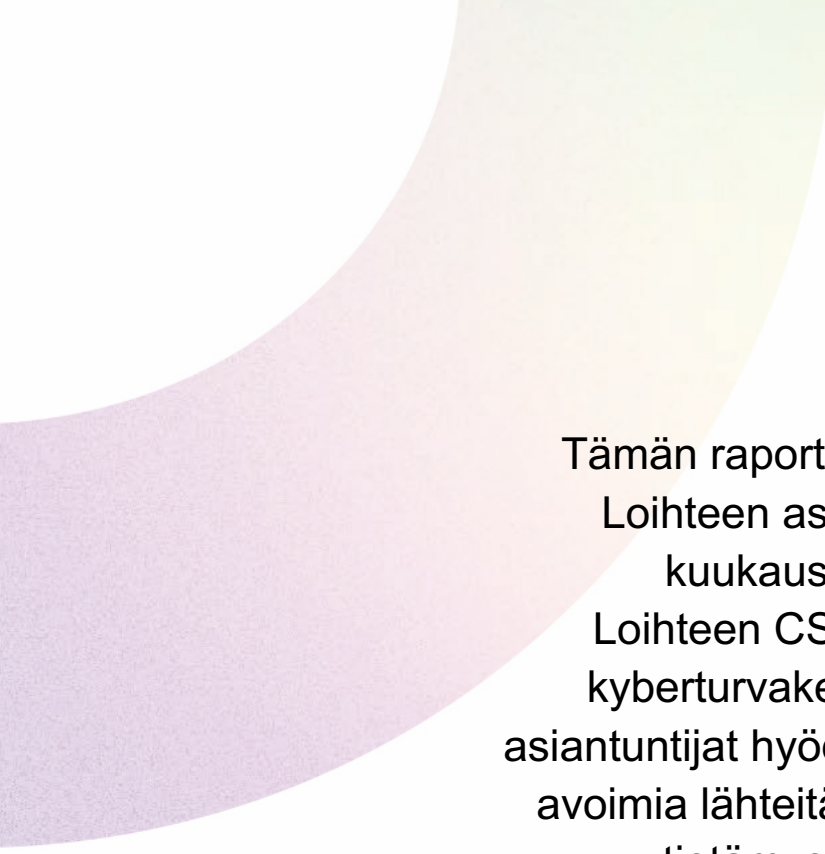
- 1 Nimeä haavoittuvuustiedotteiden seurannalle vastuuhenkilö ja varahenkilö, jotka reagoivat tiedotteisiin saman päivän aikana
- 2 Määrittele ja harjoittele hätäpäivytysprosessi, joka ohittaa normaalin huoltoikkunan
- 3 Tarkista päivityksen jälkeen mahdolliset murren merkit, sillä päivitys ei välttämättä poista jo saatua jalansijaa

Syyskuun kyberkatsaus tiivistää sen, mistä Loihteen CSOC on kirjoittanut koko vuoden: Organisaation julkiverkkoon näkyvät reunalaitteet ovat uhkatoimijoiden ensisijainen sisääntuloreitti. Pelkästään syyskuun aikana mm. seuraaviin tuotteisiin julkaistiin kriittisiä tietoturva haavoittuvuuksia, joiden hyväksikäyttö alkoi jo ennen kuin korjaavaa päivitystä oli edes saatavilla: Citrix NetScaler, F5 BIG-IP APM, Cisco ISE, Cisco Secure Email Gateway ja SonicWall SMA1000.

Ensimmäinen suositus koskee sitä, kuka organisaatiossa ylipäätään havaitsee haavoittuvuuksiin liittyvät tiedotteet. Syyskuussa SonicWall vahvisti SMA1000-tuotteen haavoittuvuuksien CVE-2026-83548 ja CVE-2026-83549 julkistamisen yhteydessä, että niitä on jo aktiivisesti hyväksikäytetty. Kyberturvallisuuskeskuksen julkaiseman F5:n CVE-2026-94127-varoituksen ilmestyessä hyväksikäyttö oli myös jo vahvistettu. Kun hyökkäykset ovat käynnissä jo haavoittuvuustiedotteen ilmestyessä, järjestelmiä ylläpitävän tahon pitää pystyä reagoimaan niihin välittömästi. Suosittelemme nimeämään haavoittuvuustiedotteiden seurannalle vastuuhenkilön ja varahenkilön, jotka käyvät valmistajien ja tiedotteet läpi päivittäin myös loma-aikana ja joilla on valtuudet käynnistää hätäpäivytysprosessi. Vastuuhenkilö tarvitsee ajantasaisen tiedon julkiverkkoon näkyvistä laitteista ja niiden versioista, jonka kartoittamista suositteelimme toukokuun Kyberkatsauksessa.

Toinen suositus koskee prosessia. Monissa organisaatioissa päivitykset asennetaan sovitun huoltoikkunan aikana, usein kerran kuussa ja iltaisin. Aktiivisesti hyväksikäytetyn haavoittuvuuden kohdalla tämä tahti on liian hidas. Hätöpäivitysprosessissa on sovittu etukäteen, kuka saa päättää huoltoikkunan ohittamisesta, mikä kriteeri sen laukaisee (esimerkiksi valmistajan vahvistama hyväksikäyttö tai Kyberturvallisuuskeskuksen varoitus), kenelle katkosta viestitään ja miten muutos kirjataan. Prosessi kannattaa myös harjoitella: valitaan yksi reunalaite ja viedään päivitys läpi hätämenettelyllä rauhallisena päivänä. Samalla selviää, onko laitteesta varmuuskopio, toimiiko palautus ja ovatko ylläpitotunnukset jonkun saatavilla myös loma-aikaan. Valmistajien väliaikaiset suojaukset, kuten F5:n tarjoama iRule-sääntö, kuuluvat samaan työkalupakkiin, ja niiden käyttöönotto on syytä osata ennen kuin sitä tarvitaan.

Kolmas suositus on se, joka jää monesti tekemättä. Tapauksissa, joissa haavoittuvuutta on hyväksikäytetty ennen korjauksen julkaisua, päivityksen asentaminen paikkaa haavoittuvuuden, mutta ei välttämättä poista jo saatua jalansijaa. Cisco Email Gatewayn tapauksessa hyökkääjän on mahdollista saada root-oikeudet tietynlaisen sähköpostiviestin lähettämällä ja tällaisella jalansijalla luodut backdoorit, lisätyt tunnukset tai muutetut konfiguraatiot säilyvät päivityksen yli. Päivityksen jälkeen laite on siksi käytävä läpi hyväksikäytön merkkien varalta valmistajan tai viranomaisen ohjeiden mukaan. F5:n tapauksessa Kyberturvallisuuskeskus neuvoo kiinnittämään huomiota OAuth-virheisiin, epäilyttäviin komentoihin ja TMM-prosessin ongelmiin. Yleisemmin kannattaa tarkistaa laitteen paikalliset käyttäjätilit, ajastetut taskit ja konfiguraation muutoshistoria sekä verrata laitteelta lähtenyt liikennettä normaaliin. Mikäli merkkejä löytyy tai lokit eivät riitä sulkemaan murtoa pois, laite on turvallisinta asentaa uudelleen puhtaasta imagesta ja vaihtaa kaikki tarvittavat salaisuudet.



Tämän raportin koostaa
Loihteen asiakkaille
kuukausittain
Loihteen CSOC:n eli
kyberturvakeskuksen
asiantuntijat hyödyntäen sekä
avoimia lähteitä että omaa
tietämystään.

Kellon ympäri miehitetty
kyberturvakeskuksemme valvoo
ja reagoi tietoturvatapahtumiin
pitäen huolen siitä, että
asiakkaamme voivat rauhassa
keskittyä liiketoimintaansa.

