



Kyberkatsaus

06/2026

LOIHDE



Tiivistelmä

Kesäkuun kyberkatsauksessa on nostettu esille kiinnostavia poimintoja ajankohtaisista tapahtumista kyberkentällä:

- Check Pointin Remote Access VPN -tuotteessa julkaistiin vakava tietoturvaavaoittuvuus, joka on jo kohdannut aktiivista hyväksikäyttöä.
- FortiGate-palomuurien admin-tunnuksia on vuodettu maailmalle yli 74000 palomuurista. Jäljet viittaavat vanhoista haavoista sekä brute force -hyökkäyksistä haltuun saatuihin tunnuksiin.
- Business intelligence -yhtiö Klue oli tietoturvahyökkäyksen kohteena, jonka seurauksena monien heidän asiakkaidensa Salesforce-instansseista saatiin anastettua tietoja.
- Anthropicin Fable- ja Mythos 5 -kielimalleista poistettiin vientikiellot ja ainakin Fable asetetaan jälleen saataville heinäkuun alusta.
- Kesäkuun tietoturvasuosituksiset liittyvät OAuth-sovellusten käyttöoikeuksiin ja niiden suojaamiseen.

KUUKAUSIRAPORTTI 06/2026

Tämä raportti sisältää poimintoja kesäkuun 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 06/2026	2
1. Poiminnat	3
1.1 CVE-2026-50751 - User Authentication bypass on VPN Remote Access and Mobile Access in deprecated IKEv1 key exchange	3
1.2 FortiBleed	3
1.3 Klue:n tietoturvapoikkeama	4
1.4 Claude Mythos ja Fable 5	4
2. Suositukset	5

1. Poiminnat

1.1 CVE-2026-50751 - User Authentication bypass on VPN Remote Access and Mobile Access in deprecated IKEv1 key exchange

Check Point julkaisi 8.6. haavoittuvuustiedotteen ja korjaavan päivityksen liittyen kriittiseen haavoittuvuuteen, joka vaikuttaa valmistajan Remote Access VPN- ja Mobile Access -ratkaisuihin. Haavoittuvuus vaikuttaa konfiguraatioihin, jotka käyttävät vanhentunutta IKEv1-protokollaa. Haavoittuvuutta hyväksikäyttämällä uhkatoimijan on mahdollista muodostaa VPN-yhteys ilman salasanaa. Check Pointin mukaan haavoittuvuus on jo kohdannut aktiivista hyväksikäyttöä. Valmistajan mukaan toistaiseksi aikaisimmat viitteet hyväksikäytöstä olisivat alkaneet 7. toukokuuta ja että hyväksikäyttö olisi kasvanut kesäkuun alusta alkaen.

Mitigoivat toimenpiteet ja korjaavat päivitykset on syytä asentaa välittömästi ja haavoittuvuudelle alttiit VPN-järjestelmät on syytä tutkia hyväksikäytön varalta, koska hyväksikäyttö on alkanut jo ennen korjaavien toimenpiteiden julkaisemista.¹

1.2 FortiBleed

Tietoturvatutkija Volodymyr Diachenko raportoi 13. kesäkuuta suuresta määrästä vuodettuja admin- ja VPN-tunnuksia FortiGate-palomuuereihin. Tämä datasetti nimettiin FortiBleed:ksi, joka sisältää kirjautumistietoja ~74000:n FortiGate-palomuurin osalta ympäri maailmaa.²

Julkaistut tiedot vaikuttavat olevan peräisin vanhoista haavoittuvuuksista ja brute force -hyökkäyksistä haltuun saaduista käyttäjätiedoista. Kyseessä ei siis ole Fortinetin tuotteisiin kohdistuva uusi tietoturva haavoittuvuus.

Tietoturvayhtiö Hudson Rock on julkaissut hakukoneen, jolla voi hakea domain-tietoja ja tarkistaa, onko oman organisaation domain vuodettujen tietojen listalla.³ Myös Fortinetin PSIRT on julkaissut tiedotteen tapauksesta sekä listannut suositukset, jotka organisaatioiden on syytä käydä läpi mahdollisen tietomurron tarkistamiseksi sekä järjestelmiensä tietoturvan parantamiseksi.⁴

¹Check Point, 8.6.2026, Security Advisory – Action Required – Active Exploitation of Check Point VPN Authentication Bypass (CVE-2026-50751), <https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/>

²Volodymyr “Bob” Diachenko, 13.6.2026, Massive Fortinet/FortiGate bruteforce/active exploitation uncovered, https://www.linkedin.com/posts/vdyachenko_massive-fortinetfortigate-bruteforceactive-activity-7471222472193830913-YBDi?utm_source=share&utm_medium=member_desktop&rcm=ACoAACGhYXoBUmguM2xVfKiB10gzN9EpEUBSwQ

³Hudson Rock, 13.6.2026, FortiBleed, <https://www.hudsonrock.com/fortinet>

⁴Fortinet, 19.6.2026, Analysis of Reported Credential Compromise of FortiGate Devices, <https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices>

1.3 Klue:n tietoturvapoikkeama

Business intelligence -yhtiö Klue raportoi 12. kesäkuuta havaitsemastaan tietoturvapoikkeamasta järjestelmissään. Tutkinnan perusteella uhkatoimija on saanut pääsyn legacy-tunnukseen, jota Klue on käyttänyt integraatiopalvelussaan. Tämän seurauksena uhkatoimijan on ollut mahdollista päästä Klue:n asiakkaiden Salesforce-instansseihin ja saada niissä oleva data haltuunsa. Kyseessä on näin ollen toimitusketjuhyökkäys, koska Klue:n asiakkaiden Salesforcessa sijaitsevaa dataa on saatu anastettua.

Tietoturvayhtiö Huntress on ilmoittanut olleensa yksi uhreista. Heidän mukaansa anastettu data sisältää mm. Salesforcessa olleita yhteystietoja, tuotteiden tilaustietoja, hintoja ja Huntressin asiakkaiden myynnilliseen dataan liittyviä tietoja.⁵

Uhkatoimija nimeltään Icarus on sittemmin ilmoittanut olevansa vastuussa hyökkäyksestä ja julkaissut Klue:n leak-sivustollaan TOR-verkossa.

1.4 Claude Mythos ja Fable 5

12. kesäkuuta Yhdysvaltain hallinto määräsi vientikiellon Anthropicin edistyksellisiin Fable- ja Mythos 5 -kielimalleihin. Vientikiellon tarkoituksena oli estää pääsy kielimalleihin Yhdysvaltojen ulkopuolisilta ihmisiltä vedoten kansalliseen turvallisuuteen. Tämän seurauksena Anthropic eväsi pääsyn kielimalleihin kaikilta organisaatioilta.

Yhdysvaltain hallinto poisti vientikiellot 30. kesäkuuta ja Anthropic ilmoitti Fable 5:n palaavan maailmanlaajuisesti käyttöön heinäkuun alusta. Lisäksi tietyille yhdysvaltalaisille organisaatioille Anthropic palauttaa käyttöön Mythos 5 -kielimallin. Tähän kielimalliin on edelleen rajattu pääsy Glasswing-ohjelmaan osallistuvilla organisaatioilla.⁶

⁵Huntress, 24.6.2026, Cybercrime Breaches Klue: Salesforce Data Impacted for Many Victims, including Huntress, https://www.huntress.com/blog/klue-breach-investigation?utm_campaign=46875268-cy26-06-18-eml-multi-global-customer-all-x-x-prg-rapid_response-awareness

⁶ <https://www.anthropic.com/news/redeploying-fable-5>

2. Suositukset

- 1 Noudata Least Privilege -periaatetta OAuth-sovelluksille
- 2 Käytöstä poistuneiden tunnusten alasajo
- 3 OAuth-sovellusten säännöllinen tietoturva-auditointi

Myönnettäessä oikeuksia OAuth-sovelluksille on syytä noudattaa least privilege -periaatetta eli myöntää sovelluksille ainoastaan ne oikeudet, jotka ne välttämättä tarvitsevat. Liialliset oikeudet altistavat sovellukset väärinkäytölle ja pitkäaikaiselle jalansijalle, esimerkiksi refresh tokenien muodossa. Esimerkiksi *offline_access* -oikeus antaa sovellukselle mahdollisuuden hakea refresh tokeneita sallien pääsyn resursseihin ilman käyttäjän hyväksyntää. Tämä on hyödyllinen ominaisuus, mutta ei aina tarpeellinen ja se voi mahdollistaa väärin käytettäessä pitkäaikaisen jalansijan.⁷

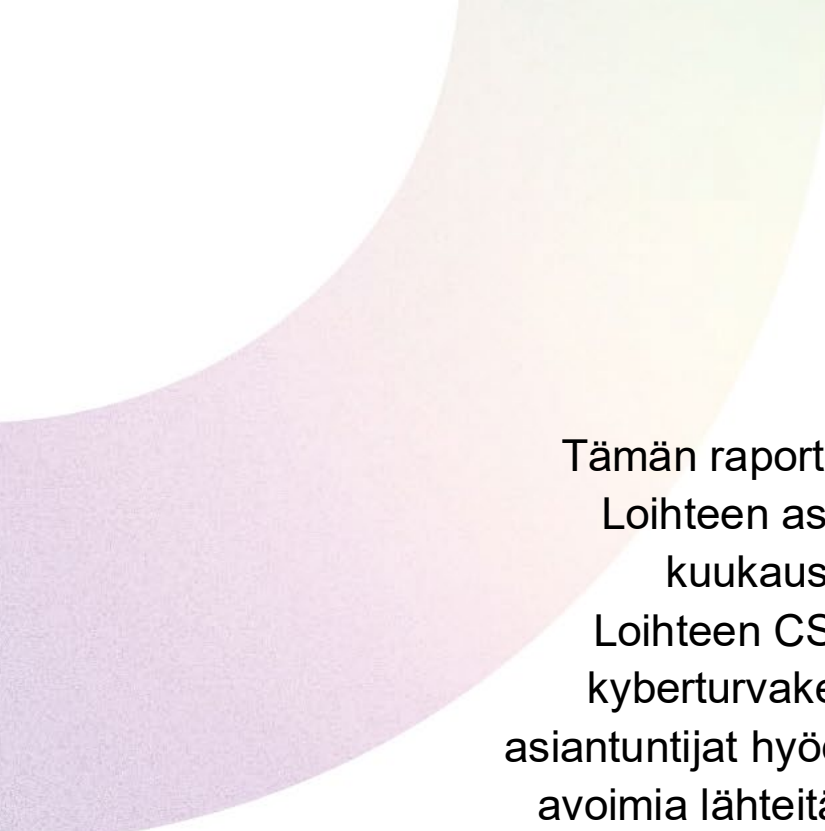
Kluen tietoturvamurrossa väitetysti hyödynnettiin pilotissa käytettyä vanhaa tunnusta, jota ei poistettu käytöstä pilotin päättymisen jälkeen. OWASP NHI Top 10 -listaa käytöstä poistuneiden NHI-tunnusten puutteellisen alasajon (Improper Offboarding) listan ensimmäisenä. Suosittelemme organisaatioita tarkastelemaan ja päivittämään prosessejaan NHI-tunnusten alasajamiseksi. Mahdollisuuksien mukaan offboardaus kannattaa myös pyrkiä automatisoimaan ja liittämään osaksi työntekijän offboardausta työsuhteen päättyessä.⁸⁹

OAuth-sovelluksia tulisi auditoida säännöllisesti ja erityisesti niille sallittuja käyttöoikeuksia tulisi tarkastella. Esimerkiksi M365-ympäristöihin saattaa jäädä lojumaan käyttämättömiä sovelluksia, joille on aikoinaan myönnetty korkeitakin käyttöoikeuksia. Applikaatioiden tarkastelu kannattaa suorittaa säännöllisesti. Organisaation OAuth-applikaatiota voi tarkastella esimerkiksi Defender for Cloud Apps -ratkaisulla. Samaa ratkaisua voidaan hyödyntää sovellusten epäilyttävän käytön havainnointiin sekä hälytyksiin.

⁷ <https://www.waldosecurity.com/post/the-oauth-permission-that-could-compromise-your-entire-org>

⁸ <https://owasp.org/www-project-non-human-identities-top-10/2025/1-improper-offboarding/>

⁹ <https://nhimg.org/faq/how-do-organisations-make-saas-offboarding-actually-work/>



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.

