Microsoft parandas juunis rekordilise arvu turvavigu ja see puudutab kõiki Windowsi kasutajaid

4 kuud tagasi - 26.06.2026 Autor: AM

(Sisuturundus)

Microsoft andis juuni 2026 Patch Tuesday raames välja uuendused ligi 200 turvanõrkuse kõrvaldamiseks, mis on ettevõtte ajaloo suurim igakuine paikamise maht. Krebsonsecurity andmetel said ligi kolm tosinat haavatavust ettevõtte kõrgeima, kriitilise raskusastme hinnangu, ning vähemalt kolme vea ärakasutamiseks on avalik exploitkood juba levinud.

Mida see tähendab neile, kes kasutavad Windowsi päris raha käsitlevates seansides

Poker Guru toimetus jälgib, kuidas eestikeelsed mänguhuvilised teevad oma esimesi samme veebipokkeri maailmas. Inimesed, kes otsivad juhiseid teemal kuidas pokkeri mängimist alustada, loovad sageli esimest korda ühenduse reaalajas toimivate platvormidega, kus liiguvad ka pärisrahalised tehingud. Seetõttu ei ole küberturvalisusega seotud riskid pelgalt teoreetilised. Kui avalikuks tulevad kriitilised haavatavused ja nende ärakasutamiseks vajalik exploit-kood levib kiiresti, muutuvad võimalikud ohud väga reaalseks.

Toimetuse hinnangul peaks enne kasutajakonto loomist või esimese deposiidi tegemist tähelepanu pöörama ka seadme turvalisusele. Arvuti või muu kasutatav seade tuleks hoida täielikult uuendatuna ning valida pokkeriplatvorm, mis suhtub operatsioonisüsteemide turvalisusesse vastutustundlikult. Nii saab veebipokkeriga alustada märksa teadlikumalt ja turvalisemalt.

Tehisintellekt kiirendab veaotsingut ja tõstab paikamiste mahtu

Rekordarvu taga on struktuurne muutus. Microsoft kirjutas eelmisel kuul avaldatud blogipostituses, et nii ettevõtte enda insenerid kui ka laiema

turvakogukonna liikmed kasutavad vigade leidmiseks üha rohkem tehisintellekti tööriistu. See tähendab, et haavatavused avastatakse kiiremini ja avalikustatakse suuremas mahus.

Tenable'i vanemteadur Satnam Narang toob konkreetse mõõdiku.

“Some surveys put AI usage among security professionals generally at 90%, so it's unsurprising that this volume of patches may be the norm. Pandora's proverbial box has been opened, and as more advanced AI models become available, we expect the norm to continue upward across the board, not just for Patch Tuesday.”

Narangi sõnum on selge: rekordmaht ei ole erand, vaid uus lähtejoon. Praktiline näide sellest suundumusest on CVE-2026-49160, teenusekatkestuse haavatavus Microsoft IIS veebiserveri tarkvaras, mille avastas ja raporteeris OpenAI Codex. Tehisintellekt ei otsi enam üksnes inimuurijate abiga, vaid iseseisvalt.

Nightmare Eclipse'i kampaania ja lubatu juuli 14. kuupäevaks

Juunikuu paikamiste seas on mitmeid nõrkusi, mille taustalugu on eriti terav. Nightmare Eclipse nimelise uurija avaldatud kaks exploiti sunnivad tähelepanu pöörama konkreetsetele vigadele. GreenPlasma kasutab ära Windows Collaborative Translation Frameworki õiguste eskalatsiooni nõrkust, mis paikati kui CVE-2026-45586. YellowKey sihtmärgiks on BitLockeri viga CVE-2026-50507, mis võimaldab füüsilise juurdepääsuga ründajal vaadata krüptitud andmeid.

Microsoft avaldas mõlema CVE nõuandes standardse tänu turvakogukonnas osalejatele, kuid ei nimetanud Nightmare Eclipse'i nimepidi. Ettevõtte sõnastus oli mõlemas adviisoris ühetaoline: "Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure." Nimetu tänamine on tähelepanuväärne, sest Nightmare Eclipse väidab end olevat endine Microsofti töötaja, kuid see väide on kontrollimata.

Veelgi muretsemapanev on uurija järgmine samm. Vahetult pärast juunikuu paikamiste avaldamist lisas Nightmare Eclipse avalikult exploiti väidetava Windows Defenderi nullpäeva jaoks ning on teatanud, et 14. juulil 2026, järgmisel Patch Tuesday kuupäeval, avaldab täiendava "bone shattering" nullpäevade komplekti. Visual Studio Code'i eraldi nullpäev, mis võimaldab ründajal ühe klikiga

varastada GitHub'i žetoone, on samuti juunikuu pildi osa. Microsoft oli sunnitud 3. juunil 2026 avaldama kiirparanduse pärast seda, kui uurija lasi juhised välja, viidates Microsofti varasemale praktikale parandada teatatud viga vaikselt ja ilma tunnustuseta.

Paikamiste tegelik ulatus ületab ametlikud arvud mitmekordselt

Ligi 200 haavatavust on märkimisväärne arv, kuid kogu pilt on laiem. Rapid7 uurija Adam Barnetti sõnul paikati juunis eraldi 360 brauseri haavatavust, mis jäävad Patch Tuesday ametlikust loendist täielikult välja.

“So far this month, Microsoft has provided patches to address 360 browser vulnerabilities, which is an order of magnitude more than has been typical in any given month over the past few years. As usual, browser [flaws] are not included in the Patch Tuesday count above. Indeed, the vast, and presumably sustained, uptick in the number of browser vulnerabilities has led to Microsoft no longer enumerating Chromium CVEs in the Security Update Guide.”

Sellele lisandub Shai-Hulud ussi puhang, mis nakatas vähemalt 72 Microsofti avalikku koodirepositooriumi. Kõik nakatunud paketid olid seotud Microsoft Azure Durable Task SDK-ga, mis langes sama ussi ohvriks juba mais. Google parandas 3. juunil 2026 avaldatud Chrome'i uuendusega 429 haavatavust. Chrome laeb uuendused küll automaatselt alla, kuid nende aktiveerimiseks on vaja brauser täielikult taaskäivitada. Adobe avaldas samuti juunis kriitilisi parandusi toodetele Experience Manager, Acrobat Reader ja ColdFusion.

Krebsonsecurity soovitab enne paikamiste paigaldamist alati teha süsteemist täielik varukoopia. Nightmare Eclipse'i lubadus täiendavate nullpäevade kohta 14. juuliks annab sellele soovitusele täiendava kaalukuse: aeg paikamiseks on praegu, mitte pärast järgmist raundet.

- Uudised
- Sisuturundus

Pilt

