jamk

NIST NVD

Ryhmä 3

Anthony Bäckström

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Harjoitustyö

Huhtikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto

Tässä harjoituksessa on tarkoituksen selvittää NIST NVD -tietokannasta tietyillä termeillä löydettyjä tuloksia. Tuloksia vertaillaan CVSS- pisteisiin sen versiossa 3.x. Jos luokassa ”critical” on useampi kuin yksi tulos, selvitetään onko niillä yhteistä nimittäjää.

Kysymykset, joihin tulee vastata. Mikä on haun pohjalta vakavin haavoittuvuus? Onko yhteistä nimittäjää? Miksi uhka on erityisen vaarallinen?

2 Haun tulokset

2.1 Reverse shell

CVE-2021-42645. CMSimple_XH 1.7.4 on altis etäkoodin suorittamiselle (remote code execution, RCE), kun hyökkääjä käyttää "File"-parametria lähettääkseen PHP-payloadin, joka mahdollistaa reverse shellin saamisen haavoittuvasta isännästä. Tämä haavoittuvuus on erittäin vaarallinen, koska se mahdollistaa hyökkääjän suorittaa mielivaltaista koodia palvelimella. Se voi johtaa järjestelmän täydelliseen komprometointiin, käyttäjätietojen varastamiseen tai jopa palvelunestohyökkäyksiin. Haavoittuvuuden vakavuus korostuu, kun otetaan huomioon CMSimple_XH:n suosio pienten ja keskisuurten verkkosivustojen keskuudessa, mikä lisää potentiaalisten kohteiden määrää.

2.2 Session poisoning

CVE-2023-47143, oli haun ainoa kriittinen haavoittuvuus. IBM Tivoli Application Dependency Manager oli haavoittuvainen HTTP header injektioille. Haavoittuvuutta voi hyödyntää mm. cross-site scriptingiin, välimuistin myrkyttämiseen (cache poisoning) tai istuntojen kaappaamiseen. Haavoittuvuus oli laaja koska se ajoittui versioiden 7.3.0.0 ja 7.3.0.10 väliin, joten se on ehtinyt olla olemassa pidemmän aikaa. Vaarallisen haavoittuvuudesta tekee se, että se on mahdollistanut mm. sivustojen väärän ohjaamisen sekä haitallisen tiedon lisäämisen sivustoille. Näillä keinoilla voidaan pyrkiä esimerkiksi tietovuotoihin.

2.3 Unisys stealth

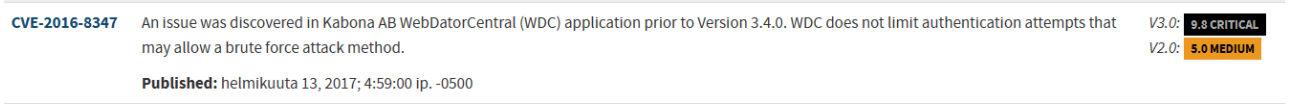
CVE-2020-12053, ainoa kriittinen haavoittuvuus. Mahdollisti pääsyn verkkoon, jos sertifikaatti pohjaista todennusta käytettiin ilman https-salattua yhteyttä. Oli verkon endpointtiin mahdollista autentikoida yhteys ilman private-keytä. Vaarallista, koska mahdollistaa luvattoman pääsyn verkon endpointtiin. Vaarallista koska altistaa mm. käyttöoikeuksiin pääsyn ja sitä kautta mahdollisuuteen esim. tietojen varastamiseen tai verkkoliikenteen sekoittamiseen.

2.4 Cisco 2950

CVE-2005-4826, tämä oli haun ainoa kriittinen löydös. Kyseessä on määrittelemätön haavoittuvuus Cisco IOS 12.1(22)EA3:n VLAN Trunking Protocol (VTP) toiminnossa Catalyst 2950T kytkimissä, joka mahdollistaa etähyökkääjien aiheuttavan palveluneston (denial of service, DoS) kohdelaitteessa lähettämällä muotoillun Subset-Advert viestipaketin. Tämä on erityisen vaarallista, koska se voi aiheuttaa verkon laitteiden uudelleenkäynnistyksiä ilman ennakkovaroitusta, häiriten merkittävästi verkon toimintaa ja palveluiden saatavuutta. Haavoittuvuus korostaa verkkoinfrastruktuurin komponenttien merkitystä kokonaisvaltaisen kyberturvallisuuden kannalta, erityisesti kun otetaan huomioon, että kytkimet ovat kriittisiä verkon toiminnan kannalta.

2.5 Brute force attempts limit

CVE-2016-8347 oli vakavin uhka CVSS 3.0 mukaan (9.8 CRITICAL). Tämä haavoittuvuus liittyy Kabona AB:n WebDatorCentral(WDC) sovellukseen ennen versiota 3.4.0. Uhka on erityisen vaarallinen koska se mahdollistaa brute force hyökkäykset. Hyökkääjät voivat toistuvasti yrittää arvata käyttäjätunnuksia ilman että järjestelmä estää yrityksiä. Tämäntyyppinen haavoittuvuus voi olla erityisen haitallinen yrityksille, joilla on paljon käyttäjiä tai jotka käsittelevät arkaluonteisia tietoja.



Kuvio 1. CVSS 3.0

CVSS 3.1 luokituksen mukaan uhat CVE-2023-33868, CVE-2022-32515, CVE-2022-2457, CVE-2021-43958 ja CVE-1999-1324 olivat vakavimpia (9.8 CRITICAL). Näissä kaikissa ja yllä olevassa uhassa oli yhteisenä nimittäjänä epäonnistuneiden kirjautumisyritysten määrän rajoituksen puuttuminen. Niin kuin yllä olevassa Kabona AB:n tapauksessa, mahdollistaa tämä hyökkääjälle brute force hyökkäykset.

CVE-2023-33868	The number of login attempts is not limited. This could allow an attacker to perform a brute force on HTTP basic authentication. **Published:** heinäkuuta 06, 2023; 7:15:09 ip. -0400	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)
CVE-2022-32515	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause brute force attacks to take over the admin account when the product does not implement a rate limit mechanism on the admin authentication form. Affected Products: Conext™ ComBox (All Versions) **Published:** tammikuuta 30, 2023; 6:15:10 ip. -0500	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)
CVE-2022-2457	A flaw was found in Red Hat Process Automation Manager 7 where an attacker can benefit from a brute force attack against Administration Console as the application does not limit the number of unsuccessful login attempts. **Published:** elokuuta 10, 2022; 4:15:36 ip. -0400	*V3.1:* 9.8 CRITICAL *V2.0:*(not available)
CVE-2021-43958	Various rest resources in Fisheye and Crucible before version 4.8.9 allowed remote attackers to brute force user login credentials as rest resources did not check if users were beyond their max failed login limits and therefore required solving a CAPTCHA in addition to providing user credentials for authentication via a improper restriction of excess authentication attempts vulnerability. **Published:** maaliskuuta 15, 2022; 9:15:07 ip. -0400	*V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH
CVE-1999-1324	VAXstations running Open VMS 5.3 through 5.5-2 with VMS DECwindows or MOTIF do not properly disable access to user accounts that exceed the break-in limit threshold for failed login attempts, which makes it easier for attackers to conduct brute force password guessing. **Published:** joulukuuta 31, 1999; 12:00:00 ap. -0500	*V3.1:* 9.8 CRITICAL *V2.0:* 7.5 HIGH

Kuvio 2. CVSS 3.1