CENTER FOR CYBERSIKKERHED

Dato: 21. juli 2016
Trusselsvurderingsenheden

Trusselsvurdering: Hjemmesider, som benytter CGI-scripts, kan være sårbare overfor kompromittering af kommunikationen til eksterne servere

Formålet med denne trusselsvurdering er at varsle om en sårbarhed, som gør det muligt for en angriber at kompromittere hjemmesider, som benytter CGI-scripts.
CFCS har set scanninger efter sårbare hjemmesider, efter sårbarheden blev offentliggjort.

Trusselsvurderingen er rettet mod ejere, administratorer og udviklere af hjemmesider.

Hovedvurdering

- CFCS vurderer, at det er MEGET SANDSYNLIGT, at ondsindede aktører vil forsøge at udnytte sårbarheden. Dette bekræftes også af, at CFCS siden offentliggørelsen, har set scanninger efter sårbarheden.
- CFCS vurderer, at den korte tid der er gået siden offentliggørelsen af sårbarheden betyder, at sårbare hjemmesider endnu ikke er blevet opdateret til at imødegå udnyttelse af sårbarheden.
- CFCS anbefaler alle ejere, administratorer og udviklere af hjemmesider snarest muligt at undersøge om deres hjemmeside er sårbar overfor denne trussel, samt at eventuelt sårbare hjemmesider snarest muligt opdateres.

Analyse

Sårbarheden

Den 18. juli 2016 blev der på internettet offentliggjort en sårbarhed, som er navngivet ”httpoxy”. Sårbarheden betyder, at en angriber kan modificere en forespørgsel mod en webserver, hvorved de forespørgsler som webserveren laver mod andre servere, bliver omdirigeret til en server, som angriberen kontrollerer. Sårbarheden eksisterer kun i de tilfælde, hvor webserveren benytter et

såkaldt Common Gateway interface (CGI), eller CGI lignende script til at kommunikere med den eksterne server.

Sårbarheden opstår, når koden i webserveren ukritisk videresender data i http-forespørgsler mod hjemmesiden videre til CGI-scriptet. Det er således muligt at sende en modificeret http-forespørgsel til webserveren, som ændrer værdien af en såkaldt environment variabel kaldet ”HTTP_PROXY”. Værdien af denne variabel kan tolkes af et CGI-script som hostname eller ip-adresse til den eksterne server, som webserveren kommunikerer med. Sårbarheden vedrører således webserverens kommunikation med en anden server via http og ikke brugerens direkte kommunikation med en given webserver.

På internettet er det muligt at finde yderligere information om sårbarheden, for eksempel via https://Httpoxy.org

Udnyttelse af sårbarheden

Udnyttelse kan for eksempel ske på en hjemmeside, som udsender vejrudsigter. Hvis en bruger ønsker vejrudsigten for en bestemt by, kan brugeren indtaste navnet på byen på hjemmesiden. Webserveren (hjemmesiden) sender så en forespørgsel til en ekstern server, som returnerer den relevante vejrudsigt til webserveren, som derefter sender vejrudsigten til brugerens browser. Kommunikationen mellem webserveren og serveren med vejrudsigten foregår typisk via et såkaldt Application Programming Interface (API) som beskriver, hvorledes webserveren skal kommunikere med applikationen på den eksterne server for at få den rigtige vejrudsigt præsenteret.

Webserveren vil typisk skulle logge ind på den eksterne server med vejrudsigter for at kunne benytte tjenesten. Da login-oplysningerne nu er sendt til den server, som angriberen kontrollerer, har angriberen nu både brugernavn og password til tjenesten.

Ovenstående eksempel er forholdsvis uskadeligt, men hvis der i stedet for en hjemmeside med vejrudsigter, er tale om en hjemmeside som indeholder data, som er kritiske for brugeren, eller håndterer betalingsoplysninger eller lignende, så kan konsekvenserne af en kompromittering være alvorlige. Det vil for eksempel være muligt for angriberen at sende skadelig kode til webserveren eller brugerens browser, at manipulere med de oplysninger som sendes til webserveren, og i sidste ende brugeren, ligesom angriberen potentielt vil have mulighed for at aflure betalingsoplysninger.

Det er relativt let for en angriber at scanne hjemmesider for at se, om de er sårbare overfor denne type angreb, og CFCS har allerede set scanninger efter denne sårbarhed på internettet i Danmark.

At en hjemmeside er sårbar betyder ikke nødvendigvis, at sårbarheden kan udnyttes af angriberen. Muligheden for at udnytte sårbarheden vil blandt andet afhænge af hjemmesidens

funktion, hvordan den er kodet, de oplysninger som hjemmesiden håndterer samt om webserveren er beskyttet af en firewall.

Common Vulnerability and Exposure registreringer

Foreløbig er følgende CVE'er registret i forbindelse med denne sårbarhed:

- CVE-2016-5385
- CVE-2016-5386
- CVE-2016-5387
- CVE-2016-5388
- CVE-2016-1000109
- CVE-2016-1000110

Hvem er ramt af sårbarheden?

På nuværende tidspunkt er der ikke overblik over, hvilke hjemmesider der er sårbare. Der er dog nogle grundlæggende kriterier, som skal være opfyldt, for at en hjemmeside er sårbar:

- Hjemmesiden skal kommunikere med andre servere, og denne kommunikation skal foregå ved hjælp af CGI- eller CGI lignende scripts.
- Koden på den angrebne webserver skal acceptere den modificerede http-meddelelse og videresende den til CGI-scriptet.

Fjernelse af sårbarheden

Via hjemmesiden https://Httpoxy.org vil det være muligt at få oplysninger om, hvordan man kan undersøge, om ens hjemmeside er sårbar overfor denne type angreb, samt hvordan man bedst kan konfigurere sin webserver til at imødegå angreb.

Endvidere bør ejere af hjemmesider være opmærksomme på, om der udsendes sikkerhedsopdateringer til den software, som benyttes på deres webservere, som imødegår de konkrete sårbarheder (CVE numre), som er listet ovenfor.

FE bruger denne skala for sandsynlighed i analyser: