CENTER FOR CYBERSIKKERHED

Dato: 31. marts 2017

Trusselsvurdering: Zero-day sårbarhed i Microsoft Windows IIS 6.0 webservere

Formålet med denne trusselsvurdering er at varsle om en alvorlig zero-day sårbarhed i IIS 6.0 webservere, som er baseret på Windows Server 2003 eller Windows XP Professional.

Hovedvurdering

- Webservere baseret på Windows Server 2003 R2 eller Windows XP Professional, indeholder software med en alvorlig zero-day sårbarhed. I Danmark findes der tusindevis af disse webservere. Microsoft opdaterer ikke længere softwaren.
- Det er sandsynligt, at ondsindede aktører vil forsøge at udnytte sårbarheden.

Analyse

På internettet er der for nylig offentliggjort en alvorlig sårbarhed i softwaren Microsoft Internet Information Services (IIS) 6.0. IIS 6.0 er en webserver, som blev leveret sammen med Windows server 2003 R2 samt Windows XP Professional x64 Edition.

Sårbarheden har en CVSS (version 2.0) score på 10, som er det højest mulige. Sårbarheden kan relativt let udnyttes via internettet, og kræver ikke login.

Sårbarheden, som har identiteten CVE-2017-7269, er en såkaldt ”buffer overflow” sårbarhed i WebDAV funktionen. WebDAV gør det muligt for web-redaktører at samarbejde om indholdet på en hjemmeside. Sårbarheden kan udnyttes ved, at en aktør sender særligt udformede kommandoer til webserveren, som gør aktøren i stand til at eksekvere kode på webserveren.

På internettet er der offentliggjort exploits, som viser, hvordan sårbarheden kan udnyttes. Konsekvensen af en succesfuld udnyttelse af sårbarheden kan være uautoriseret adgang til information på webserveren eller afbrydelse af webserveren.

En scanning af internettet tyder på, at der i Danmark er flere tusinde ISS 6.0 webservere, som potentielt er sårbare. Udnyttelse af sårbarheden kræver imidlertid, at WebDAV funktionen er aktiveret på webserveren, hvilket den ikke er som standard. Undersøgelser tyder på, at det globalt set kun er omkring 10 % af webserverne, som har WebDAV aktiveret.

Microsoft ophørte med at udsende sikkerhedsopdateringer til Windows server 2003 samt Windows XP den 14. juli 2015, og derfor kan softwaren indeholde flere sårbarheder, som ikke er blevet fjernet via sikkerhedsopdateringer.

Anbefaling
CFCS anbefaler, at administratorer af Microsoft Windows servere og webservere undersøger, om de benytter software, som indeholder sårbarheden, og i pågældende tilfælde deaktivere WebDAV funktionen.

CFCS anbefaler generelt virksomheder og myndigheder til ikke at benytte software, som ikke længere modtager sikkerhedsopdateringer fra leverandøren. Dette gælder især i de tilfælde, hvor den pågældende software benyttes til systemer, som kan nås via internettet.

Nye sårbarheder i software og it-systemer opdages konstant. Hvis leverandøren ikke løbende udsender sikkerhedsopdateringer som fjerner disse sårbarheder, eller hvis brugeren ikke implementerer disse sikkerhedsopdateringer, vil softwaren eller it-systemet udgøre en sikkerhedsrisiko for brugeren.

FE bruger denne skala for sandsynlighed i analyser: