Security Advisory Response - Log4j / CVE-2021-44228

Van toepassing op: Visma | Raet & Visma | YouServe

14-12-2021

Visma | Raet & Visma | YouServe

Plotterweg 38
3821 BB Amersfoort
+31 88 23 02 300

Laarderhoogtweg 17
1101 DZ Amsterdam

Lavendelheide 7a
9202 PD Drachten

security.raet@visma.com
security.youserve@visma.com

Security Advisory

Op vrijdag 10-12-2021 is een kwetsbaarheid gepubliceerd in Apache Log4j2 < 2.14.1 waar geen patch voor beschikbaar was, een zogenoemde 0-day kwetsbaarheid. Deze kwetsbaarheid is dermate ernstig dat succesvol misbruik kan leiden tot Remote Code Execution.

Youforce

Na het publiceren van de kwetsbaarheid is op 10 december direct door Visma Security een inventarisatie gedaan van Youforce systemen die Java en/of Log4j gebruiken. Uit deze inventarisatie is naar voren gekomen dat Youforce applicaties *géén* gebruik maken van kwetsbare Log4j libraries.

Visma .net HRM en Payroll

Na het publiceren van de kwetsbaarheid is tevens een inventarisatie gedaan van Visma .net HRM en Payroll systemen. Uit deze inventarisatie is naar voren gekomen dat Visma .net HR en Payroll applicaties *géén* gebruik maken van kwetsbare Log4j libraries.

Leveranciers

Naast door onszelf ontwikkelde systemen maken wij ook gebruik van systemen van leveranciers. Wij hebben contact met al deze leveranciers. Zodra leveranciers een advisory plaatsen met een update of workaround voor hun product volgen wij die na interne beoordeling op. Zo hebben wij afgelopen weekend direct een update uitgevoerd voor Ping Identity zodra deze beschikbaar was.

Vervolgstappen

Om het risico nog verder te mitigeren hebben we onder andere een detectie-regel in onze eigen security monitoring toegevoegd om pogingen tot misbruik van CVE-2021-44228 automatisch te detecteren en blokkeren. Verder is door onze security partners (Qualys, Tenable, Fox-IT, F5 & Visma CSIRT) al gecommuniceerd dat ook zij actieve detectie-regels hebben ingericht tegen misbruik van deze kwetsbaarheid.

Door alle mitigerende acties zijn onze systemen niet kwetsbaar voor de Log4j/Log4Shell kwetsbaarheid. Uiteraard blijven wij de situatie monitoren en nemen wij direct actie waar dat nodig is.