Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

NUCLEUS:13 - Mehrere Schwachstellen im Netzwerkstack "Nucleus"

Nr. 2021-269348-1022, Version 1.0, 09.11.2021

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Sicherheitsforscherinnen und -forscher der Firmen Forescout Research Labs und Medigate Labs haben dreizehn Schwachstellen in den Implementierungen des TCP/IP-Stacks "Nucleus NET" gefunden. Der Netwerkstack ist eine Komponente des Nucleus RTOS (Nucleus Real-Time Operating System), einem 1993 von Accelerated Technology (AT) erstmals veröffentlichten Echtzeitbetriebssystem. 2002 übernahm Mentor Graphics das Unternehmen. Seit 2017 gehört Mentor Graphics zum Siemens-Konzern. Der Netzwerkstack wird von verschiedensten anderen Herstellern für Produkte in den Bereichen Medizingeräte, Automotive und Operational Technology (OT) eingesetzt, in denen besondere Anforderungen an Safety und Security gestellt werden.

Die unter den Namen NUCLEUS:13 [FOR2021d] veröffentlichen Schwachstellen beschreiben unter anderem mehrere fehlende Validierungen der Länge von Datenfeldern in TCP-, UDP-, ICMP- und DHCP-Paketen, das Verarbeiten maliziöser TCP-Pakete und TFTP-Befehle sowie weitere Schwachstellen im Zusammenhang mit der FTP-Implementierung. Die veröffentlichten Schwachstellen können deshalb zum Eingriff in den Speicher der Endsysteme genutzt werden.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Als Resultat können auf den Endgeräten ein Denial of Service (DoS) erzwungen, eigener Code eingeschleust und ausgeführt (RCE), ICMP-Antworten an Dritte gesendet oder Speicherinformationen des Systems (Information Leak) ausgelesen werden.

Es handelt sich um Schwachstellen, die die komplette Lieferkette betreffen. Betroffen sind unter anderem die Produkte:

- Capital VSTAR
- Nucleus NET
- Nucleus ReadyStart
- Nucleus RTOS

Der Hersteller des Stacks hat Updates bereitgestellt [SIE2021]. Diese müssen durch Firmen, die den Stack wiederum in ihren Produkten nutzen, noch eingebunden und aktualisierte Versionen bereitgestellt werden. Forescout verlinkt in seinem GitHub-Repository zum Projekt Memoria Advisories von Herstellern [FOR2021e]. Diese Liste erhebt jedoch keinen Anspruch auf Vollständigkeit.

Die in NUCLEUS:13 gefundenen Schwachstellen sind vergleichbar mit den bereits veröffentlichten Schwachstellen AMNESIA:33 (siehe [FOR2020a], [JSF2021], [BSI2020]), NUMBER:JACK [FOR2021a], NAME:WRECK [FOR2021b] und INFRA:HALT [FOR2021c].

Bewertung

Aufgrund der weiten Verbreitung, dem Schadenspotenzial und da es sich bei den Netzwerkstacks um zentrale Komponenten der Produkte handelt, stuft das BSI die Schwachstellen als grundsätzlich relevant ein.

Derzeit liegen dem BSI keine Hinweise darauf vor, dass eine oder mehrere der oben genannten Schwachstellen bereits aktiv ausgenutzt werden.

Betreiber können in der aktuellen Lage fast ausschließlich mitigierende Maßnahmen ergreifen, da die meisten Schwachstellen nur über Updates der Gerätehersteller zu beseitigen sind. Da die Softwareversion und die Herkunft des in Geräten verwendeten TCP/IP-Stacks oft nicht leicht herauszufinden ist, kann deren Betroffenheit zudem nur schwer ermittelt werden.

Maßnahmen

Das BSI empfiehlt jedem Betreiber zu überprüfen, ob Produkte im Einsatz sind, die durch die Schwachstellen betroffen sind und die beschriebenen Maßnahmen der Hersteller bezüglich Updates und dem sicheren Betrieb der Systeme zeitnah zu berücksichtigen. Sollten Sie OT-Geräte verwenden, kann Fragen zur Betroffenheit eines Produktes **ausschließlich der Hersteller beantworten.**

Des Weiteren empfiehlt das BSI folgende Maßnahmen umzusetzen:

1. Erzwingen Sie Segmentierungskontrollen und eine ordnungsgemäße Netzwerkhygiene, um das Risiko anfälliger Geräte zu verringern. Beschränken Sie externe Kommunikationspfade und isolieren Sie anfällige Geräte in Zonen als mitigierende Maßnahme.
2. Stellen Sie sicher, dass DHCP Antworten von nicht-autorisierten Servern geblockt oder verworfen werden.
3. Überwachen Sie den Netzwerkverkehr auf Anomalien und verwerfen Sie ungültige Pakete.
4. Deaktivieren oder blockieren Sie nicht verwendete / benötigte Protokolle in den kritischen Netzwerksegmenten (bspw. FTP, TFTP)

Darüber hinaus sollten Industrielle Steuerungssysteme (ICS) nicht direkt aus dem Internet erreichbar sein, sondern durch eine konsequente Anwendung der Defense-in-Depth-Strategie geschützt werden. Allgemeine Hinweise zur Absicherung von ICS stellt das BSI im ICS-Kompendium [BSI2013] sowie auf der offiziellen BSI Webseite [BSI2021] bereit.

Links

[BSI2013] BSI ICS-Security Kompendium
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html

[BSI2020] AMNESIA33: Teils kritische Schwachstellen gefunden
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Amnesia_201208.html

[BSI2021] Industrielle Steuerungs- und Automatisierungssysteme (ICS)
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/industrielle-steuerungs-automatisierungssysteme_node.html

[FOR2020a] Advisory AMNESIA:33
https://www.forescout.com/research-labs/amnesia33/

[FOR2021a] NUMBER:JACK - Forescout Research Labs Finds Nine ISN Generation Vulnerabilities Affecting TCP/IP Stacks
https://www.forescout.com/company/blog/numberjack-forescout-research-labs-finds-nine-isn-generation-vulnerabilities-affecting-tcpip-stacks/

[FOR2021b] NAME:WRECK - RESEARCH REPORTBreaking and fixing DNS implementations
https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/

[FOR2021c] INFRA:HALT -RESEARCH REPORT
https://forescout.com/research-labs/infra-halt/

[FOR2021d] NUCLEUS:13 -RESEARCH REPORT
https://www.forescout.com/research-labs/nucleus-13/

[FOR2021e] Project Memoria - Advisories
https://github.com/Forescout/project-memoria-advisories/blob/main/advisories.md

[SIE2021] SSA-044112: Multiple Vulnerabilities (NUCLEUS:13) in the TCP/IP Stack of Nucleus RTOS
https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.