



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Schwachstelle "NAME:WRECK" betrifft mehrere DNS- Implementierungen

CSW-Nr. 2021-207948-1032, Version 1.0, 19.04.2021

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

Sicherheitsforscher der Firma JSOF und der Forescout Research Labs haben neun Schwachstellen in den DHCP und DNS-Implementierungen der TCP/IP-Stacks von vier Betriebssystemen gefunden, welche vorwiegend in Echtzeitkommunikationen eingesetzt werden.

Die unter den Namen NAME:WRECK [FOS2021, JSF2021] veröffentlichten Schwachstellen beschreiben mehrere fehlerhafte Validierungsmechanismen von Datenfeldern in DNS-Antwortpaketen, welche zum Eingriff in den Speicher der Endsysteme genutzt werden können.

Als Resultat kann auf dem Endgeräten ein Denial of Service (DoS) erzwungen, oder eigener Code eingeschleust und ausgeführt werden (Remote Code Execution RCE).

Betroffen von diesen Schwachstellensind vier Systeme, zu unterschiedlichen Anteilen:

1. **FreeBSD:** Wird häufig in Computern, Druckern und Netzwerkgeräten in der Device Cloud verwendet.
2. **IPNet:** Integrierte-Lösung von IPNet Solutions für Unternehmens- und Telekommunikationsmärkte.
3. **NetX:** Zu den gängigen Produktkategorien gehören Mobiltelefone, Unterhaltungselektronik und Geschäftsautomatisierung in Geräten wie Druckern, intelligenten Uhren, Systemen auf einem Chip sowie Energie- und Stromversorgungsanlagen in industriellen Steuerungssystemen (ICS).

* 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.

4. **Nucleus NET:** Teil von Nucleus RTOS und in über 3 Milliarden Geräten implementiert. Wird häufig in der Gebäudeautomation, in der Betriebstechnologie und in VoIP sowie in Ultraschallgeräten, Speichersystemen und kritischen Systemen für die Avionik verwendet.

Die genaue Betroffenheit der einzelnen Stacks können dem Bericht von Forescout [FOS2021] entnommen werden.

Grundsätzlich wird zur Ausnutzung der Schwachstellen eine privilegierte Rolle im Netzwerk oder der Kommunikation benötigt, um Endgeräten mit manipulierten DNS-Paketen antworten zu können. Diese Rolle kann durch einen kompromittierten Server sowie einem sogenannten "Man in the Middle" Angriff erlangt werden. Sollte es einem Dritten gelingen, eine solche Rolle einzunehmen, ist das Netzwerk auch ohne die unter NAME:WRECK aufgeführten Schwachstellen essentiell gefährdet.

Bewertung

Das BSI geht aufgrund der Verbreitung in verschiedenen Branchen von einer grundsätzlichen Relevanz aus. Derzeit liegen dem BSI keine Hinweise darauf vor, dass eine oder mehrere der oben genannten Schwachstellen bereits aktiv ausgenutzt werden. Jedoch existieren bereits Proof-of-Concepts zur Ausnutzung dieser Schwachstellen.

Da es sich bei DNS um ein essentielles System handelt, ist ein erhöhtes Interesse seitens der Angreifer an der Kompromittierung von DNS-Servern und -Resolvern anzunehmen.

Maßnahmen

Das BSI empfiehlt jedem Betreiber zu überprüfen, ob die betroffenen Produkte im Einsatz sind und die beschriebenen Maßnahmen der Hersteller bezüglich Updates und dem sicheren Betrieb der Systeme zeitnah zu berücksichtigen. Zur Ermittlung, ob eines der verwundbaren Systeme im Einsatz ist, stellt Forescout diverse Skripte [GIT2021] zur Verfügung.

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 alle exponierten DNS-Systeme entsprechend den Hersteller- und Sicherheitsvorgaben betrieben werden und nicht von Schwachstellen betroffen sind.
3. Nutzen Sie für sämtliche ausgehenden DNS-Anfragen einen internen DNS-Resolver. Dies ermöglicht es, den DNS-Verkehr zu überprüfen.
4. Überwachen Sie den externen DNS-Datenverkehr, um frühzeitig Kompromittierungsversuche zu erkennen und setzen Sie sich bei verdächtigem externen DNS-Datenverkehr zeitnah mit Ihrem Provider in Verbindung.

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] bereit.

Links

[FOS2021] Advisory NAME:WRECK DNS Vulnerabilities

<https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/>

[GIT2021] Github Skript um NAME:WRECK DNS Schwachstellen zu erkennen

<https://github.com/Forescout/project-memoria-detector>

[JSF2021] JSOF Blogpost to NAME:WRECK DNS Vulnerabilities

<https://www.jsf-tech.com/namewreck-dns-vulnerabilities-disclosed-by-jsf-and-forescout/>

[BSI2013] BSI ICS-Security Kompendium

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompodium_pdf.html

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 sensiblen 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.